Military Science and Tactics
AJA Command and Staff University
https://www.qjmst.ir/
Online ISSN: 4520-2676
Print ISSN: 2008-191x

The Correct Behavioral Pattern of Information Security Employees in the Face of Cyber Security Threats With the Mediating Role of Policy and Organizational Culture

Mohammad Bagher Raen Abromand[1] | Sedigheh Mohammad Esmaeil✉[2] | Dariush Matlabi[3]

1. Ph. D. student in Information Science and Epistemology, Islamic Azad University Research Science Unit, Tehran, Iran.
Email: ITmanager@tsfc. ir
2. Corresponding author: Associate Professor, Department of Information Science and Epistemology, ResearchSciences Unit,Islamic Azad University, Tehran. Iran.
Email: Sm. esmaili2@gmail. com
3. Associate Professor, Department of Educational Sciences, Yadgar Imam Khomeini (RA) Shahrari Unit, Islamic Azad University, Tehran, Iran.
Email: dariushmatlabi@yahoo. com

Article Info

Article type:

Research Article

Article history:

Received

28 May 2023

Received in revised form

19 September 2023

Accepted

30 September 2023

Published online

11 September 2025

Keywords:

Behavioral¬pattern, information security, cyber threats,hybridization, organizational culture

ABSTRACT

Objective: In this research, the effective factors on the behavior of information security employees were investigated and the role of organizational culture on the behavioral pattern of employees was determined and an optimal behavioral pattern was proposed.

Methodology: The research analyzed the factors affecting the behavioral pattern in the face of cyber security threats using a combined method, and the effect of policy and organizational culture on it was investigated with a meta-composite (sequential-exploratory) method.

Findings: First, 270 primary sources including domestic and foreign articles were screened and 83 domestic sources and 29 foreign sources were selected. From these sources, 142 indicators consisting of 5 dimensions and 17 components were extracted, then with the help of the two-stage Delphi method, the questions were evaluated and validated, and 11 indicators were removed from them, and in the quantitative stage, a questionnaire with 131 questions was created. It was prepared and information security experts answered the questionnaire.

Conclusion: By analyzing the data using SPSS and MATLAB software. It was found that there is a statistically significant relationship between the two characteristics of policy and organizational culture and the behavior pattern of information security experts in relation to information security policy.

Cite this article: Raen Abromand, M. B. , Mohammad Esmaeil, S & Matlabi, D. (2025). The correct behavioral pattern of information security employees in the face of cyber security threats with the mediating role of policy and organizational culture. *Military Sciences and Techniques*, 21(72), 35-68.
DOI: http//doi. org/ 10. 22034/qjmst. 2025. 2010648. 1941

CC BY NC ND

Publisher: AJA Command and Staff University
DOI: 10. 22034/qjmst. 2025. 2010648. 1941

فصلنامه علمی علوم و فنون نظامی
شاپای چاپی: ۱۹۷۸-۲۰۰۸ شاپای الکترونیکی: ۲۶۷۶-۴۵۲۰ https://www.qjmst.ir/ دانشگاه فرماندهی و ستاد آجا

الگوی رفتاری صحیح کارکنان امنیت اطلاعات در مواجه با تهدیدات امنیتی سایبری با نقش میانجی خط‌مشی و فرهنگ سازمانی

محمدباقر رایین آبرومند[۱] | صدیقه محمداسماعیل[۲]✉ | داریوش مطلبی[۳]

۱. دانشجو دکتری تخصصی علم اطلاعات و دانش‌شناسی واحد علوم و تحقیقات دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: ITmanager@tsfc. ir

۲. نویسنده مسئول، دانشیار گروه علم اطلاعات و دانش‌شناسی واحد علوم و تحقیقات دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: Sm. esmaili2@gmail. com

۳. دانشیار گروه علوم تربیتی، واحد یادگار امام خمینی(ره) شهرری، دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: dariushmatlabi@yahoo. com

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی
تاریخ دریافت:
۱۴۰۲/۰۳/۰۷
تاریخ بازنگری:
۱۴۰۲/۰۶/۲۸
تاریخ پذیرش:
۱۴۰۲/۰۷/۰۸
تاریخ انتشار:
۱۴۰۴/۰۶/۲۰
کلیدواژه‌ها:
الگوی رفتاری، امنیت اطلاعات، تهدیدات سایبری، فراترکیب، فرهنگ سازمانی

چکیده

هدف: در این پژوهش عوامل موثر بر رفتار کارکنان امنیت اطلاعات بررسی گردید و نقش فرهنگ سازمانی بر الگوی رفتاری کارکنان مشخص شد و یک الگوی رفتاری بهینه پیشنهاد گردید.

روش‌شناسی: پژوهش به روش ترکیبی به تحلیل عوامل موثر بر الگوی رفتاری در مواجه با تهدیدات امنیتی سایبری پرداخته و با روش فراترکیب (متوالی-اکتشافی) اثر خط¬مشی و فرهنگ سازمانی بر آن مورد بررسی قرار گرفته است.

یافته‌ها: ابتدا ۲۷۰ منبع اولیه شامل مقالات داخلی و خارجی غربالگری گردید و ۸۳ منبع داخلی و ۲۹ منبع خارجی انتخاب شد. از این منابع، ۱۴۲ شاخص مشتمل بر ۵ بعد و ۱۷ مولفه استخراج گردید، سپس به کمک روش دلفی دو مرحله‌ای، سوالات ارزش‌سنجی و روایی‌سنجی شده و از این میان ۱۱ شاخص حذف شدند و در مرحله کمی یک پرسشنامه با ۱۳۱ سوال آماده گردید و کارشناسان امنیت اطلاعات به پرسشنامه پاسخ دادند.

نتایج: با تحلیل داده‌ها به کمک نرم افزارهای SPSS و MATLAB. مشخص گردید که بین دو ویژگی خط‌مشی و فرهنگ سازمانی و الگوی رفتاری کارشناسان امنیت اطلاعات نسبت به سیاست امنیت اطلاعات از نظر آماری رابطه معناداری وجود دارد.

استناد: رایین آبرومند، محمدباقر؛ محمداسماعیل، صدیقه و مطلبی، داریوش. (۱۴۰۴). الگوی رفتاری صحیح کارکنان امنیت اطلاعات در مواجه با تهدیدات امنیتی سایبری با نقش میانجی خط‌مشی و فرهنگ سازمانی. *علوم و فنون نظامی*، ۲۱(۷۲): ۶۸- ۳۵.
DOI: http//doi. org/ 10. 22034/qjmst. 2025. 2010648. 1941

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران.

CC BY NC ND

DOI: 10. 22034/qjmst. 2025. 2010648. 1941

Military Science and Tactics
AJA Command and Staff University
https://www.qjmst.ir/
Online ISSN: 4520-2676
Print ISSN: 2008-191x

The Correct Behavioral Pattern of Information Security Employees in the Face of Cyber Security Threats With the Mediating Role of Policy and Organizational Culture

Mohammad Bagher Raen Abromand[1] | Sedigheh Mohammad Esmaeil[2] | Dariush Matlabi[3]

Extended Abstract

Introduction

Today, the success of information security depends to a large extent on effective user behavior. Correct and constructive behaviors of users, system administrators, and other individuals can greatly enhance the effectiveness of information security; while incorrect and destructive behaviors can actually hinder its effectiveness. Given that the complexities of human factors affect the availability, reliability, and integrity of information systems. Given the general lack or lack of research in this field and given the importance of information security for today's organizations and the direct impact of human factors management on the organization's information security, the present study aims to present a different approach to information security by focusing on "behavioral information security, professionals, and managers" and by identifying and examining the obvious and hidden factors affecting information security in organizations, to present a model of correct professional behavior for information security experts in the face of cyber threats with quantitative and qualitative assessments. Among the vectors for reducing data-related attacks and incidents, the present study highlights the importance of defining a cybersecurity awareness plan that includes providing training to employees and using simulation scenarios to identify social engineering and phishing campaigns. (1) Employees can acquire the cybersecurity skills necessary to effectively manage and respond to cybersecurity threats and risks. In this way, employees can gain a proper understanding of the cybersecurity threats and risks that companies face and gain greater confidence in managing cybersecurity tasks. (2)

Methodology

In the present study, with a combined (sequential-exploratory) approach, data from documentary studies were collected and analyzed qualitatively and the meta-synthesis method (a method based on a systematic review of library studies) was used to identify the components of the appropriate behavioral pattern of information security experts. The meta-synthesis method consists of two basic parts: qualitative and quantitative. In the qualitative part, new and basic topics and metaphors were explored, and the components of the appropriate behavioral pattern of information security experts were extracted from internal and external sources. The experts' perspectives were used to confirm the desired components. Therefore, experts constitute the qualitative statistical population of this study.

Findings

In the first round, the validity of the indicators for Delphi was examined with the help of 15 experts, including nine information security professors and six information technology professors, all of whom had doctoral degrees. In the second round, the indicators that were agreed upon by the experts in the first round of Delphi were provided to the second group of experts to be evaluated. In the second round, electronic and paper questionnaires were provided to 15 people. The educational degree of the experts studied in the second round of Delphi was a master's degree in information technology and information security, and after the final analysis, the indicators were evaluated and the indicators outside the evaluation were eliminated. The criteria for evaluating the indicators were the CVR (content validity ratio) and CVI (content validity index) parameters, and indicators with a CVR above 74% and a CVI above 49% were approved. (Balan et al. 2020) In total, according to Table (2),

the final questionnaire approved by the experts was prepared, including 5 dimensions and 17 indicators, and out of 142 indicators extracted from the sources, 131 indicators were finally approved.

Dimensions and components of research in cyber threats

Dimensions	Component
Security Vulnerabilities	Insufficient protection against eavesdropping/interception and criminal activity
	Unauthorized physical access
	Weakness in maintaining information resources
	Defects in information infrastructure
Security Threats	Criminal activity service blockage
	Physical threats
	Unintentional damage
	Misuse
Human Factors	Administrative
	Application
Process Factors	Rules
	Monitoring
Technical Factors	Planning
	Equipment
	Encryption
	Monitoring
	Access control

The study used three criteria of reliability, convergent validity and divergent validity. It is necessary to examine the reliability at the representative and latent variable levels. Representative reliability was examined by measuring factor loadings and the reliability of latent variables was examined through composite reliability. In the table below, the Cronbach's alpha value for all variables is greater than the appropriate limit of 0/6 and they have a desirable reliability.

Calculating Cronbach's alpha, reliability, composite reliability, and variance of research dimensions and components

Mean Explained Variance AVE>0/5	Composite Reliability CR>0/7	Reliability rho_A>0/7	Cronbach's Alpha CA>0/6	Hidden variables	
0/763	0/995	0/997	0/994	Cyber threats	
0/817	0/991	0/991	0/991	Security vulnerabilities	1
0/864	0/981	0/978	0/977	Inadequate protection against eavesdropping/interception and criminal activity	1-1
0/888	0/96	0/944	0/937	Unauthorized physical access	1-2
0/866	0/978	0/974	0/974	Weakness in maintaining information resources	1-3
0/821	0/97	0/964	0/964	Defects in information infrastructure	1-4
0/803	0/991	0/991	0/991	Security threats	2
0/88	0/983	0/981	0/981	Denial of service	2-1
0/918	0/971	0/956	0/955	Criminal activity	2-2
0/854	0/981	0/979	0/979	Physical threats	2-3

Military Science and Tactics
AJA Command and Staff University
https://www.qjmst.ir/
Online ISSN: 4520-2676
Print ISSN: 2008-191x

Mean Explained Variance AVE>0/5	Composite Reliability CR>0/7	Reliability rho_A>0/7	Cronbach's Alpha CA>0/6	Hidden variables	
0/847	0/978	0/974	0/974	Inadvertent damage	2-4
0/797	0/983	0/982	0/982	Misuse	3
0/836	0/973	0/967	0/967	Human factors	3-1
0/834	0/976	0/972	0/971	Management	3-2
0/775	0/982	0/981	0/981	Application	4
0/834	0/976	0/972	0/971	Process factors	4-1
0/821	0/974	0/97	0/969	Laws	4-2
0/719	0/969	0/991	0/965	Monitoring	5
0/591	0/882	0/762	0/889	Technical factors	5-1
0/865	0/983	0/981	0/98	Planning	5-2
0/89	0/985	0/982	0/982	Equipment	5-3
0/535	0/902	0/905	0/887	Cryptography	5-4
0/883	0/984	0/982	0/981	Monitoring	5-5

Conclusion

The origin of an organization's policy is the organization's rules, and the result of the policy is achieving the organization's goals. The high weight of the "rules" index in the "process factors" component and the need to update the policy, which is one of the characteristics of the "rules" index, indicates the importance of the policy and organizational culture. The high weight of the indicators related to organizational culture in the "human factors" dimension indicates the direct and influential relationship of organizational culture on the behavioral pattern of information security experts. Therefore, organizational policy and culture play a significant role in correcting or destroying the behavioral pattern of information security experts and, consequently, in the organization's performance. Errors in the information security policy can directly affect the organization's performanc

پرتال جامع علوم انسانی

This page is intetionally blank

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

مقدمه

اطلاعات با ارزش‌ترین دارایی سازمان محسوب می‌شود و به دلیل ارزش بالا و حیاتی آن، باید از آن به خوبی محافظت شود. برخی از نخبگان اطلاعات را به خون در رگ‌های سازمان تشبیه نموده‌اند که عامل حیات‌بخش محسوب می‌شود و در صورت محدودیت یا به خطر افتادن این جریان، سازمان با مرگ مواجه خواهد شد. برنامه‌ریزی راهبردی و اقدام هدفمند نسبت به اطلاعات سازمان، نقش حیاتی در اجتناب از هدر دادن فرصت‌ها، دوباره کاری، اتلاف منابع و عدم سازگاری سیستم‌های اطلاعاتی دارد و می‌تواند فرصتی برای بهره‌برداری صحیح از فرصت‌های ناشی از اطلاعات را به همراه داشته باشد. این امر چالشی برای بالا بردن کیفیت اطلاعات در سازمان از جنبه‌های صحت، وجود در زمان مناسب، کامل بودن، اعتماد به منشاء اعتبار و مناسب بودن را ایجاد می‌نماید، اطلاعات اغلب برای هدایت فرآیندهای کسب و کار و کارکنان از سطوح عالی تا عملیاتی کاربرد دارد و بدون شک مدیریت اثربخش اطلاعات موجب مزیت رقابتی و ارزش برای سازمان گشته و سهام‌داران و سرمایه گذاران را خشنود می‌سازد (رحیملی و علیار، ۱۳۹۱).

با نگاهی به سند راهبردی امنیت فضای تبادل اطلاعات کشور و با استناد به بند ج ماده ۴۴ قانون برنامه چهارم و پنجم توسعه اقتصادی، اجتماعی، فرهنگی و علمی کشور پرداختن به امنیت تبادل اطلاعات به عنوان یک ضرورت و اولویت تلقی شده است. در سال ۲۰۲۱، در سراسر جهان سازمان‌ها حدود ۱۵۰ میلیارد دلار برای امنیت سایبری هزینه کردند که سالانه ۱۲. ۴ درصد رشد می‌کند. نظرسنجی از ۴۰۰۰ شرکت متوسط نشان می‌دهد که حجم تهدیدها از سال ۲۰۲۱ تا ۲۰۲۲ تقریباً دو برابر شده است. بر اساس این نظرسنجی، تقریباً ۸۰ درصد از گروه‌های تهدید مشاهده‌شده فعال در سال ۲۰۲۱ و بیش از ۴۰ درصد از بدافزارهای مشاهده‌شده، قبلاً هرگز دیده نشده بودند. تحقیقات نشان می‌دهد که ۷۰٪ از تقلب توسط خودی‌ها و نه توسط مجرمان خارجی انجام می‌شود، اما ۹۰٪ از کنترل‌های امنیتی و نظارت بر تهدیدات خارجی متمرکز است (کول ویل[1] ۲۰۰۹)، این موضوع نشان‌دهنده خطای ساختاری و فرهنگ ناصحیح سازمانی بوده و بیانگر آن است که همچنان نیاز به اصلاح خط‌مشی و تصحیح ساختار سازمانی احساس می‌شود. از سوی دیگر، تصمیم‌گیری فرآیندی بسیار مهم و پایه‌ای در فعالیت‌های مدیران است که اساس آن به دست آوردن و پردازش اطلاعاتی می‌باشد که باید سه

[1] Colwill

صفت محرمانگی، صحت و در دسترس بودن را داشته باشد، در غیر این صورت خسارات بزرگی برای سازمان به بار می‌آید. امنیت اطلاعات مبحث بسیار مهمی است؛ زیرا هدف آن حفاظت از اطلاعات سازمان در برابر تهدیدها و ریسک‌ها در دسترسی کاربران به اطلاعات امن، مطمئن و محرمانه است و برای اطمینان از امنیت آن، سازمان باید سیاست‌ها و خط‌مشی‌های امنیت اطلاعات را شناسایی و تبیین کند. شکست‌های مداوم امنیت اطلاعات در سازمان‌ها باعث تمرکز بیشتر بر فرهنگ سازمانی شده است. همچنین یکی دیگر از نگرانی‌های بزرگ برای امنیت اطلاعات یک سازمان، رفتار کارکنان است زمانی که برای سیاست امنیت اطلاعات ارزش قائل نیستند و از آن مهم‌تر رفتار کارشناسان امنیت اطلاعات می‌باشد و عدم رعایت سیاست‌های امنیتی سیستم‌های اطلاعاتی کارشناسان امنیت اطلاعات یک نگرانی عمده برای مدیران امنیت فناوری اطلاعات می‌باشد (کریمی و پیکری، ۱۳۹۸).

استدلال می‌شود که توسعه فرهنگ امنیت اطلاعات متعاقباً به یک سازمان امن منجر خواهد شد. با این حال مطالعات محدودی برای درک فرهنگ امنیت اطلاعات انجام شده است. فرهنگ ایده آل یا قوی امنیت اطلاعات می‌تواند در به حداقل رساندن تهدید انسان‌ها به حفاظت از اطلاعات و در نتیجه کمک در کاهش نقض داده‌ها یا حوادث در سازمان‌ها کمک کند. تقریباً همه سازمان‌ها اطلاعات حساس را به شکلی جمع‌آوری و نگهداری می‌کنند. برخی از سازمان‌های دولتی کنترل‌های نظارتی بر استفاده و توزیع انواع خاصی از اطلاعات حساس ایجاد کرده‌اند. برخی از سازمان‌های جنایی با مهارت‌های فنی بهبود یافته سازمان‌دهی می‌شوند و مصمم هستند که به‌طور غیرقانونی انواع خاصی از اطلاعات حساس را برای سود خود به دست آورند. خطرات مرتبط با از دست دادن اطلاعات حساس یک نگرانی بسیار واقعی برای سازمان‌های امروزی است. اگر اشتباهی در الگوی رفتاری یا استانداردهای اخلاقی یک کارشناس امنیت اطلاعات وجود داشته باشد، ممکن است منجر به از دست دادن شهرت یا کاهش مزیت رقابتی برای سازمان شود (الهوگیل[1] ,۲۰۱۵).

سازمان‌ها به سیاست‌ها و شیوه‌های امنیت اطلاعات برای ایجاد مدیریت مناسب و استفاده از اطلاعات حساس به منظور کاهش خطرات مرتبط نیاز دارند. سیاست‌های امنیت اطلاعات فقط به اندازه افرادی که باید آنها را اعمال کنند موثر هستند (نیکرک و سولمز[2] ,۲۰۰۵). فرهنگ یک سازمان تأثیر زیادی بر ارزش‌ها، اسطوره‌ها، قهرمانان و نمادهای کارمندان دارد که برای

[1] AlHogail
[2] Niekerk & Solms

کارمند معنا می‌بخشد (دیل و کندی[1], ۱۹۹۹). این امکان وجود دارد که سیستم‌ها و نمادهای ارزش فرهنگی بتوانند بر نگرش کارکنان نسبت به سیاست‌های امنیت اطلاعات سازمان تأثیر بگذارند. در بسیاری از سازمان‌ها، خط‌مشی‌ها و رویه‌های سیستم امنیت اطلاعات دارای عنصری از انطباق کارکنان است که برای اطمینان از راه‌حل امن‌تر مورد نیاز است. این برای پاسخگویی به تهدیدات مداوم پیشرفته‌ای که دارایی‌های اطلاعاتی ارزشمند سازمان را هدف قرار می‌دهد، مورد نیاز است. هنگامی که یک روش حمله کشف و متوقف می‌شود، روش دیگری راه اندازی می‌شود. ماهیت غیرقابل پیش‌بینی تهدیدات مداوم پیشرفته برای اطلاعات حساس سازمان، نیاز به راه حل‌های تطبیقی را معرفی می‌کند. وابستگی پذیرفته شده به پذیرش و انطباق کارشناسان امنیت اطلاعات با سیاست‌ها و رویه‌های امنیت اطلاعات سازمان نشان می‌دهد که نیاز به درک بهتر تأثیرات احتمالی بر پذیرش و انطباق کارکنان وجود دارد. هدف از این مطالعه رسیدن به الگوی صحیح رفتاری کارشناسان امنیت اطلاعات نسبت به سیاست امنیت اطلاعات در مواجهه با تهدیدات امنیتی و سایبری است.

پیشینه پژوهش

جرایم سایبری یکی از رایج‌ترین فعالیت‌هایی است که افراد به منظور آسیب رساندن به سازمان‌ها و سرقت داده‌ها، اسناد و اطلاعات مهم بانکی انجام می‌دهند (قربانی و ثقفی، ۱۳۹۸). یافته‌های تجی و محمد (۲۰۲۳) نشان می‌دهد که انسجام گروهی، آگاهی امنیت اطلاعات و شیوه‌های کاری غیررسمی، تأثیر قابل توجهی بر فرهنگ امنیت اطلاعات دارد. علاوه بر این، فرهنگ امنیتی تأثیر مثبتی بر درک موفقیت امنیت اطلاعات دارد. برای درک بهتر ابعادی که ممکن است بر انطباق امنیت اطلاعات کارکنان تأثیر بگذارد، شیافن[2] (۲۰۲۳) در پژوهش خود چارچوبی را معرفی می‌کند که بر اساس ترکیب نظریه‌های انگیزش و رفتار است که یافته ی‌کلیدی او عبارت است از " انطباق کارکنان امنیت اطلاعت تحت تأثیر عواملی است که این عوامل بر اساس چهار بعد متمایز عمل می‌کنند: آگاهی، انگیزه، قابلیت و فرهنگ سازمانی". علی (۲۰۲۱) در یافته‌های خود به این نتیجه رسید که تحقیقات بیشتر بر روی رفتارهای انطباقی تمرکز دارد تا رفتارهای عدم انطباقی کارکنان امنیت اطلاعات. تضادهای ارزشی، استرس مربوط به امنیت، و خنثی‌سازی، در میان بسیاری از عوامل دیگر، شواهد قابل توجهی از عدم انطباق را ارائه می‌کنند. "کارکنان انگیزه‌های داخلی و خارجی را از دایره اجتماعی،

[1] Deal & Kennedy
[2] Xiaofeng Chen

رفتارهای مدیریتی و فرهنگ سازمانی خود برای اتخاذ رفتارهای آگاهانه از امنیت درک می‌کنند. تکنیک‌های بازدارندگی، رفتارهای مدیریتی، فرهنگ و آگاهی از امنیت اطلاعات نقشی حیاتی در تبدیل عدم انطباق کارمندان به رفتارهای انطباقی دارند".

به منظور شناسایی پیوندهای مخرب(دی پیر ۱۴۰۱) در پژوهش خود معیاری برای محاسبه خطر امنیتی پیوندها ارائه نموده است. نتایج نشان دهنده کارایی معیار پیشنهادی ایشان بوده است و این معیار قادر است درصد بالایی از پیوندهای مخرب موجود در مجموعه داده‌ها را شناسایی کند. استفاده از عبارت "درصد بالایی" در پژوهش دی پیر تصدیق‌کننده این موضوع است که زیرساخت و فناوری نمی‌تواند تضمین‌کننده امنیت اطلاعات باشد و در نهایت این نیروی انسانی است که پاشنه آشیل در امنیت اطلاعات می‌باشد، بنابراین در این پژوهش بر آن شدیم که اثر عوامل مختلف بر رفتار کارکنان امنیت اطلاعات را برآورد کنیم (استانتون[1] ۲۰۰۴). در تحقیقات خود به این نتیجه رسیده اس که اگرچه راه‌حل‌های مبتنی بر فناوری به کاهش برخی از مشکلات متعدد امنیت اطلاعات کمک می‌کنند، حتی بهترین فناوری نیز نمی‌تواند با موفقیت کار کند مگر اینکه افراد سازمان‌ها کار درست را انجام دهند. با توجه به مطالعات علی (۱۴۰۰) مبنی بر اینکه استرس، موانع کاری و رفتارهای همکاران بر رفتارهای کارکنان تاثیر می‌گذارد، می‌توان اولویت بندی‌های عوامل ایجاد استرس شغلی در مطالعات حسینی (۱۳۹۳) را ملاکی برای الگوی رفتاری کارکنان در نظر گرفت، به نقل از حسینی، عوامل ایجاد کننده استرس شغلی به شرح زیر اولویت‌بندی گردید: ۱- عوامل سازمانی ۲- فرهنگ و بافت سازمانی ۳- خط‌مشی سازمانی ۴- فشار نقش‌ها ۵- عوامل ساختاری ۶- عدم امنیت شغلی / مالی ۷ -ناپایداری ۸- روابط بین فردی ۹- شایستگی نقش و ۱۰- تطبیق با شرایط شغلی. با توجه به اینکه در پژوهش حسینی، فرهنگ سازمانی و خطی مشی اولویت‌بندی دوم و سوم را دارند، بنابراین می‌توان نتیجه گرفت که خط‌مشی و فرهنگ سازمانی اثر مستقیم بر رفتار کارکنان می‌گذارد. در این خصوص ارنست[2] (۲۰۰۷) نیز در مطالعات خود به این نتیجه رسیده است که فرهنگ مناسب برای امنیت اطلاعات برای سازمان‌ها بسیار مهم است زیرا ابعاد انسانی امنیت اطلاعات را نمی‌توان به طور کامل با اقدامات فنی و مدیریتی حل کرد. نتایج یک نظرسنجی از ۵۰۰ کارمند استرالیایی نشان داد که رابطه مثبت و معنی داری بین تصمیم گیری امنیت اطلاعات و فرهنگ امنیت اطلاعات سازمانی وجود دارد. این نشان

[1] Stanton
[2] Ernest

می‌دهد که بهبود فرهنگ امنیتی یک سازمان تاثیر مثبتی بر رفتار کارکنان خواهد داشت که به نوبه خود باید انطباق با سیاست‌های امنیتی را نیز بهبود بخشد. این بدان معنی است که خطر برای سیستم‌های اطلاعاتی و داده‌های سازمان کاهش می‌یابد. سالامون[1] (۲۰۲۱) نیز در مطالعات خود به این نتیجه رسیده است که فرهنگ سازمانی و فرهنگ امنیت اطلاعات تاثیرات قابل توجهی بر انطباق کارکنان دارند. تجزیه و تحلیل نشان می‌دهد که یک شکل بوروکراتیک فرهنگ سازمانی برای تقویت انطباق سیاست‌های امنیت اطلاعات کارکنان مفید است. کارلسون[2] (۲۰۲۲) در نتایج پژوهش خود به این طبقه‌بندی دست یافته است که "فرهنگ‌سازمانی" با رتبه میانگین ۱۶. ۲۶ رتبه اول، "ساختار سازمانی" با رتبه میانگین ۱۳ رتبه دوم، "منابع انسانی" با رتبه میانگین ۱۲. ۱۱ رتبه سوم، "زیرساخت فناوری اطلاعات" با رتبه میانگین ۱۱. ۶۳ رتبه چهارم، "آموزش و بازآموزی" با رتبه میانگین ۱۰. ۹۸ رتبه پنجم و "جنبه راهبردی و رهبری" با رتبه میانگین ۹. ۴۸ در رتبه ششم قرار دارد. در نهایت مطابق جدول (۱) دو پژوهش شعبانی و حسینی از نظر اولیت‌بندی عوامل موثر بر الگوی رفتاری کارکنان، با هم مقایسه شده‌اند.

جدول (۱) مقایسه پژوهش‌های شعبانی ۱۴۰۰ و حسینی ۱۳۹۳

شعبانی (۱۴۰۰)		حسینی (۱۳۹۳)	
رتبه میانگین	مؤلفه	مؤلفه	اولویت
۲۶/۱۶	فرهنگ‌سازمانی	عوامل سازمانی	۱
۱۳	ساختار سازمانی	فرهنگ و بافت سازمانی	۲
۱۱/۱۲	منابع انسانی	خط‌مشی سازمانی	۳
۶۳/۱۱	زیرساخت فناوری اطلاعات	عوامل ساختاری	۴
۹۸/۱۰	آموزش و بازآموزی	روابط بین‌فردی	۵
۴۸/۹	جنبه راهبردی و رهبری	تطبیق با شرایط شغلی	۶

مبانی نظری

در بعضی سازمان‌ها، امنیت سایبری به طور مترادف با امنیت اطلاعات استفاده می‌شود، ولی این دو مشابه نیستند. امنیت سایبری، راهبرد، سیاست و استانداردهای مربوط به امنیت و

[1] Solomon
[2] Karlsson

عملیات در فضای سایبری بوده و از دامنه‌ای از سیاست‌ها و فعالیت‌های کاهش تهدید، کاهش‌آسیب‌پذیری، کاهش‌بازدارندگی، درگیری‌بین‌المللی، پاسخ به حادثه، تاب‌آوری و ترمیم شامل عملیات شبکه کامپیوتری، اعتماد اطلاعاتی، اعمال‌قانون، دیپلماسی، ارتش و فعالیت‌های اطلاعاتی تا جایی که به امنیت و پایداری زیر ساخت‌های اطلاعات و ارتباطات جهانی مربوط است، را دربر می‌گیرد. به‌طورکلی، امنیت سایبری، توان حفاظت یا دفاع کاربر فضای سایبری از حملات سایبری است. هر رویداد یا واقعه با قابلیت وارد نمودن ضربه به مأموریت، وظایف دستگاه متولی، سرمایه ملی سایبری یا کارکنان سازمان به‌واسطه یک سازمان اطلاعاتی از طریق دسترسی غیرمجاز، انهدام (تخریب) افشای، تغییر اطلاعات و یا ممانعت از ارائه خدمت باشد را می‌توان تهدیدات سایبری نامید (سند راهبردی پدافند سایبری کشور ۱۳۹۰).

با بررسی پیشینه پژوهش‌های انجام شده اثر خط‌مشی و فرهنگ سازمانی بر رفتار کارشناسان امنیت اطلاعات در تهدیدات سایبری کاملا مشهود گردید و پژوهش‌های ذیل نیز تایید کننده این موضوع است. همان‌گونه که فرهنگ سازمانی در هر کشور نشات گرفته از فرهنگ بومی آن کشور است پس می‌توان از خط‌مشی‌های تبیین شده در فضای مشابه در دنیا استفاده کرد ولی باید با نگاه بومی‌سازی متناسب با فرهنگ عمومی جامعه تغییراتی ایجاد کرد، برای مثال در پژوهش الشیخ[1] (۲۰۲۰)، پنج ابتکار کلیدی را که سه سازمان استرالیایی برای بهبود فرهنگ‌های امنیت سایبری مربوطه خود اجرا کرده‌اند، شناسایی و توضیح می‌دهد. پنج ابتکار کلیدی شامل: شناسایی رفتارهای کلیدی امنیت سایبری، ایجاد شبکه 'قهرمان امنیت سایبری'، توسعه یک برند برای تیم سایبری، ساخت یک مرکز امنیت سایبری، و همسو کردن فعالیت‌های آگاهی امنیتی با کمپین‌های داخلی و خارجی است. این ابتکارات کلیدی به سازمان‌ها کمک کرده است تا از حداقل استانداردها-انطباق برای ایجاد فرهنگ‌های کاربردی امنیت سایبری فراتر روند. تحقیقات فراوانی در مورد عواملی که ممکن است بر هدف انطباق با خط‌مشی کارشناسان امنیت اطلاعات تأثیر بگذارد، انجام شده است و نتایج آن متفاوت است. (پیوست ۱)

- بررسی، شناخت و اصلاح الگو رفتاری کارشناسان امنیت اطلاعات در سازمان‌های داده‌محور باعث دستیابی به:
  - شناخت الزامات امنیتی و استراتژی‌های مقابله با تهدیدات سایبری در سازمان هدف (سازمان‌های داده‌محور و فاوا محور)

[1] Alshaikh

- شناخت شرح وظایف اصلی کارشناسان امنیت اطلاعات در سازمان‌های هدف (سازمان‌های داده‌محور و فاوا محور)
- ارزیابی مستمر امنیت اطلاعات و اعمال اصلاحات مناسب در سازمان‌های هدف.
- ارائه رویکرد و چارچوب و خط‌مشی امنیت اطلاعات برای پیاده‌سازی، پایش و اصلاح که بافرهنگ سازمان سازگار باشد.
- اطمینان از رویکردی جامع برای مدیریت امنیت اطلاعات.
- پیشگیری و یا به‌حداقل‌رساندن توان آسیب‌پذیری تهدیدات سایبری در سازمان.
- آگاه‌سازی، تعلیم و آموزش مناسب

- برخی پیامدهای حاصل از خطاهای خط‌مشی امنیت اطلاعات:
  - سلب اعتماد مشتریان
  - سلب اعتماد سرمایه گذاران
  - پیامدهای قانونی به دلیل عدم ایجاد یک سیستم ایمن
  - اختلال در فرآیندهای جاری سازمان
  - از دست دادن اطلاعات و داده‌های مهم
  - خدشه به اعتبار و شهرت یک سازمان
  - افزایش هزینه

روش‌شناسی پژوهش

در پژوهش حاضر با رویکرد، ترکیبی (متوالی- اکتشافی) داده‌های حاصل از مطالعات اسنادی، به صورت کیفی جمع‌آوری و تحلیل گردیده و با روش فراترکیب (روشی مبتنی بر مرور سیستماتیک مطالعات کتابخانه‌ای) برای شناسایی مؤلفه‌های الگوی رفتاری مناسب کارشناسان امنیت اطلاعات استفاده شده است. روش فراترکیب شامل دوبخش اساسی کیفی و کمی می‌باشد که دربخش کیفی به کشف موضوع‌ها و استعاره‌های جدید و اساسی پرداخته شده و مؤلفه‌های الگوی رفتاری مناسب کارشناسان امنیت اطلاعات از منابع داخلی و خارجی استخراج گردید و برای تایید مؤلفه‌های مورد نظر از دیدگاه خبرگان استفاده شد بنابراین خبرگان جامعه آماری کیفی این پژوهش را تشکیل می‌دهند.

روش فراترکیب روشی مبتنی بر مرور سیستماتیک مطالعات کتابخانه‌ای جهت دستیابی به شناخت عمیق پیرامون پدیده مورد مطالعه است (خداکرمیان، ۱۴۰۲). فراترکیب با فراهم کردن یک نگرش نظام‌مند برای پژوهشگران از طریق ترکیب پژوهش‌های کیفی مختلف، به

کشف موضوع‌ها و استعاره‌های جدید و اساسی می‌پردازد. ازآنجایی‌که بیشتر منابع در زمینه مؤلفه‌های الگوی رفتاری مناسب کارشناسان امنیت اطلاعات، مطالعات کیفی و بدون داده‌های کمی هستند روش فراترکیب به عنوان روشی مناسب برای به دست آوردن تلفیق جامعی از این موضوع بر پایه مطالعات کیفی محدود استفاده شده است. برای گردآوری داده‌های پژوهش از پژوهش‌های انجام شده (اعم از پژوهشی و مروری) در زمینه امنیت سیستم‌های اطلاعاتی استفاده شده است به منظور شناسایی مؤلفه‌های در حوزه امنیت سیستم‌های اطلاعاتی به وسیله روش فراترکیب از روش هفت مرحله‌ای باروسو[1] و ساندلوسکی[2] ۲۰۰۷ استفاده شده است. به طور خلاصه، ابتدا تمام عوامل استخراج شده دربخش منابع داخلی و خارجی در زمینه مؤلفه‌های الگوی رفتاری نامناسب کارشناسان امنیت اطلاعات را به عنوان کد در نظر گرفته، و با در نظر گرفتن مفاهیم هر یک از مؤلفه‌ها، آنها را در یک مفهوم مشابه ابعاد دسته‌بندی می‌شود (پیوست ۱).

درادامه، به کمک اطلاعات بدست آمده پرسشنامه‌هایی تهیه گردید و بین کارشناسان و متخصصان امنیت اطلاعات توزیع گردید و به صورت کمّی وزن مولفه‌ها بدست آمده و نتیجه‌گیری نهایی حاصل شده است، بنابراین در این پژوهش با پیاده‌سازی روش دلفی و ایجاد ارتباط بین خبرگان و متخصصان نتایج کاربردی پیش‌رو برآورد گردید.

بنابر کیفی بودن ماهیت پژوهش حاضر، برای انتخاب نمونه آماری خبرگان دربخش کیفی و تعیین حجم نمونه، از روش نمونه‌گیری ترکیبی هدفمند (همگن و گلوله برفی) استفاده شده است. در نمونه‌گیری همگن، پس از بررسی دقیق و عمیق، افراد با خصوصیات مشترک انتخاب شده، و سپس با استفاده از روش گلوله برفی، با توجه به موضوع تحقیق از افراد متخصص خواسته شد تا افراد خبره و باتجربه دیگری را معرفی کنند. انتخاب افراد برای فرآیند دلفی در این پژوهش، وابسته به تجربه‌ها و تخصص‌های موردنیاز در موضوع مورد مطالعه بوده و بر اساس یک یا هردو ویژگی زیرمی‌باشد.

- ❖ مدیران واحدهای سازمانی حوزه امنیت اطلاعات
- ❖ اساتید دانشگاهی مرتبط با علم رایانش امن

از میان افراد معرفی شده، ۱۱۲ نفر از خبرگان‌بخش کیفی، واجد شرایط تشخیص داده شدند و گام بعدی، جلب مشارکت نامزدها برای مشارکت در انجام پژوهش است که به صورت حضوری،

[1] Barroso
[2] Sandelowski

تماس تلفنی و ارسال نامه الکترونیکی صورت پذیرفت. سپس دعوت نامه‌ای به همراه پرسشنامه در اختیارشان قرار گرفت که شامل چگونگی انجام پژوهش و دریافت موافقت آنها برای مشارکت بود. از این میان درمجموع ۱۵ نفر برای دور اول دلفی و ۱۵ نفر دیگر برای دور دوم دلفی تمایل و موافقت خود را برای مشارکت در کارگروه دلفی اعلام کردند. لذا در این پژوهش از تعداد ۳۰ خبره استفاده شد و پرسشنامه اولیه برای ایشان ارسال شد. لیست شرکت‌های داده‌محور و کارشناسان امنیت اطلاعات پس از فیلتر شدن با معیار حداقل ۵ سال سابقه کار مرتبط، به تعداد ۱۵۶ نفر رسیدند، با استفاده از فرمول کوکران (رابطه شماره ۱) حداقل حجم نمونه برابر ۱۱۱ نفر گردید ولی پرسشنامه‌ها به هر ۱۵۶ نفر ارسال گردید و پس از دریافت ۱۱۱ پرسشنامه تکمیل شده، فرایند تحلیل آغاز گردید و مطابق پیش‌بینی، حدود ۴۰ نفر به پرسشنامه پاسخ ندادند و یا پاسخ کامل ندادند و نیمه کاره رها کردند.

فرآیند آماده‌سازی پرسشنامه به کمک روش دلفی

از آنجائی که بسیاری از اسناد به دست آمده حاوی اطلاعات کلی در زمینه الگوی رفتاری بوده و اطلاعات مفیدی برای ایجاد مؤلفه در این حوزه ارائه نمی‌کرد، نتایج به دست آمده در این مرحله طی چند فرایند پالایش شدند تا اسناد نامرتبط مشخص شوند و اسنادی که موضوع پژوهش را کامل پوشش می‌دهند به عنوان اسناد مرتبط انتخاب شوند. در این مرحله ابتدا به روش کتابخانه‌ای ۲۷۰ سند شناسایی گردید و از ۲۷۰ سند به‌دست‌آمده، ۱۵۸ سند تحت فرایند پالایشی CASP از فرایند فراترکیب حذف شدند که نهایتاً دستاورد این مرحله از پژوهش، ۱۱۲ سند مرتبط با موضوع پژوهش حاضر بود که حاصل مرحله فراترکیب است، در نهایت ۱۴۲ سؤال به‌عنوان شاخص که با " الگوی رفتاری کارشناسان امنیت اطلاعات در مواجه با تهدیدات سایبری و امنیتی" مطابقت داشته‌اند استخراج گردید و بر اساس آن پرسشنامه‌ای مطابق با طیف لیکرت تهیه شد و به خبرگان ارسال شد.

طیف لیکرت

یکی از محبوب‌ترین مقیاس‌های کدگذاری داده‌های کیفی به صورت عددی، طیف یا مقیاس لیکرت است. به کمک این طیف یا مقیاس، پاسخ‌دهندگان به هر گویه یا شاخص، میزان موافقت خود را با موضوع مرتبط با گویه براساس سطوحی که از قبل تعیین شده، مشخص می‌کنند. معمولا تعداد پنج سطح مختلف در طیف لیکرت در نظر گرفته می‌شود. در این حالت، طیف لیکرت پنج سطحی، می‌تواند گزینه‌های، کاملاً مخالفم، مخالفم، نظری ندارم، موافقم و کاملاً موافقم را داشته باشد.

استخراج مولفه‌ها

در دور اول روایی شاخص‌ها برای دلفی با همراهی ۱۵ نفر از خبرگان بررسی شد که شامل نه استاد امنیت اطلاعات و شش استاد فناوری اطلاعات که مدرک تحصیلی همه دکتری بوده است

در مرحله دوم شاخص‌هایی که از دید خبرگان مرحله اول دلفی مورد اجماع قرار گرفته بودن، در اختیار گروه دوم خبرگان قرار گرفت تا مورد ارزیابی قرار گیرد. در دور دوم پرسشنامه‌های الکترونیکی و کاغذی در اختیار ۱۵ نفر قرار گرفت. مدرک تحصیلی خبرگان مورد مطالعه در مرحله دوم دلفی کارشناسی ارشد دررشته فناوری اطلاعات و امنیت اطلاعات بوده است و پس از تحلیل نهایی، شاخص‌ها ارزش‌گذاری شده و شاخص‌های خارج از ارزش گذاری حذف گردیدند. ملاک ارزش گذاری شاخص‌ها پارامتر CVR[1] (نسبت روایی محتوایی) و CVI[2] (شاخص روایی محتوایی) بوده است و شاخص‌های با CVR بالای ۷۴٪ و CVI بیش از ۴۹٪ مورد تایید قرار گرفته‌اند. (بالان و همکاران ۲۰۲۰) در مجموع، مطابق جدول (۲)، پرسشنامه نهایی مورد تایید خبرگان شامل ۵ بعد و ۱۷ شاخص تهیه گردید و از ۱۴۲ شاخص استخراج شده از منابع، در نهایت ۱۳۱ شاخص تایید گردیدند.

جدول (۲) لیست نهایی ابعاد و مولفه‌های پژوهش در تهدیدات سایبری

ابعاد	مولفه
آسیب‌پذیری‌های امنیتی	حفاظت ناکافی در مقابل شنود/ره‌گیری و بروز فعالیت مجرمانه
	دسترسی فیزیکی غیرمجاز
	ضعف در نگهداری منابع اطلاعاتی
	نقص در زیرساخت‌های اطلاعاتی
تهدیدات امنیتی	انسداد خدمت فعالیت مجرمانه
	تهدیدات فیزیکی
	خسارت‌های غیرعمدی
	سوء استفاده
عوامل انسانی	مدیریتی
	کاربردی
عوامل فرآیندی	قوانین
	نظارت
عوامل فنی	برنامه‌ریزی

[1] Content Validity Ratio
[2] Content Validity Index

ابعاد	مولفه
	تجهیزات
	رمز نگاری
	پایش
	کنترل دسترسی

یافته‌های پژوهش

در این پژوهش برای اعتبارسنجی مدل‌ها از تحلیل‌عاملی تاییدی و با استفاده از نرم افزار SPSS انجام شده است بنابراین پیش‌فرض اساسی آن است که هر عاملی با زیرمجموعه خاصی از متغیرها ارتباط دارد. برای ارزیابی اعتبارسنجی مدل‌های اندازه‌گیری مقادیر زیر را محاسبه کرده و در صورت برآورده شدن شرایط مندرج در جدول (۳) می‌توانیم ادعا کنیم که مدل اندازه‌گیری از شرایط مناسب و مطلوبی برقرار است.

جدول(۳) شرایط برقراری پایایی و روایی همگرا

شاخص	حد مجاز	منبع
پایایی	• پایایی ترکیبی بالاتر از ۰/۷ و آلفای کرونباخ بیشتر از ۰/۶	(جوزپ و همکاران (۲۰۱۶
روایی همگرا	• بارهای عاملی استاندارد باید بزرگتر از ۰/۵ و معنادار باشد. • CR>AVE • AVE>0/5 • Rho_A>0/6	
روایی واگرا	• AVE>MSV	
شاخص‌های برازش مدل	• SRMR<0/1 • NFI>0/9	

***AVE: Average variance Extracted, CR: Construct Reliability, MSV: Maximum Shared Squared variance, GOF; Goodness of Fit and NFI: Normed fit index**

در پژوهش حاضر، برای تعیین اتفاق نظر میان اعضای پانل علاوه بر شاخص‌های مرکزی شامل میانگین و انحراف استاندارد و. . آزمون تی-تک‌نمونه‌ای، CVI و CVR، از ضریب هماهنگی کندال نیز استفاده شده است. ضریب هماهنگی کندال با ضریب همبستگی تاو کندال تفاوت دارد. کندال در ضریب همبستگی کندال دارای خواصی نظیر ضریب همبستگی ساده است. برای برآورد آن از آماره τ استفاده می‌شود. ضریب همبستگی کندال که با نماد W نشان داده می‌شود یک آزمون ناپارامتریک است و برای تعیین میزان هماهنگی میان نظرات استفاده می‌شود. ضریب کندال بین ۰ و ۱ متغیر است. اگر ضریب کندال صفر باشد یعنی عدم توافق کامل و اگر یک باشد یعنی توافق کامل وجود دارد. ویژگی‌های ضریب کندال یکی از مهمترین

کاربردهای این آزمون را در مدیریت فراهم کرده، استفاده شده است (احمد ۲۰۰۳). نتایج دلفی نشان می‌دهد که اتفاق نظر اعضای نشست حاصل شده است و می‌توان به تکرار دوره‌ها پایان داد. با توجه به کمتر بودن مقدار سطح معنی داری از ۰/۰۵ می‌توان گفت که ضریب توافقی کندال معنادار بوده است و در سطح اطمینان ۹۵ ضریب پایایی در ارائه این ارزیابی کلی از پایایی اندازه‌گیری از ۰ تا ۱ متغیر است. اگر همه پارامترهای مقیاس کاملاً مستقل از یکدیگر باشند (یعنی همبستگی ندارند یا هیچ کوواریانسی ندارند)، $\alpha = 0$؛ و اگر همه گویه‌ها کوواریانس بالایی داشته باشند، با نزدیک شدن تعداد پارامترهای مقیاس به بی‌نهایت، α به ۱ نزدیک می‌شود. به عبارت دیگر، α بالاتر است ضریب، هرچه اقلام دارای کوواریانس مشترک بیشتری هستند و احتمالاً همان مفهوم اساسی را اندازه‌گیری می‌کنند. ٪ اتفاق نظر بین خبرگان در هر سه مرحله وجود داشته است.

آلفای کرونباخ مطابق رابطه ۲ با گرفتن امتیاز از هر پارامتر مقیاس و همبستگی آنها با نمره کل برای هر مشاهده و سپس مقایسه آن با واریانس برای تمام نمرات پارامترها محاسبه می‌شود. آلفای کرونباخ به بهترین وجه به عنوان تابعی از تعداد سؤالات یا موارد در یک معیار، میانگین کوواریانس بین جفت گویه‌ها و واریانس کلی نمره کل اندازه گیری شده درک می‌شود.

$$\propto = \frac{K}{K-1}\left(1 - \frac{\sum_{i=1}^{k} \sigma_y^2}{\sigma_x^2}\right) \qquad (2)$$

K: تعداد موارد در اندازه گیری

σ_y^2 : واریانس مرتبط با هر کدام

σ_x^2 : واریانس مربوط به کل نمرات

مطابق جدول (۴) کیفیت پایایی درونی بر حسب ضریب آلفای کرونباخ برآورد می‌گردد.

جدول (۴) کیفیت پایایی درونی بر حسب ضریب آلفای کرونباخ

ضریب آلفا کرونباخ	پایایی درونی
۰٫۹α ≥	عالی
۰٫۸ > α ≥ ۰٫۹	خوب
۰٫۷ > α ≥ ۰٫۸	قابل قبول
۰٫۶ > α ≥ ۰٫۷	مورد سؤال
۰٫۵ > α ≥ ۰٫۶	ضعیف
α۰٫۵ >	غیرقابل قبول

در بررسی مدل‌های بیرونی از سه معیار پایایی، روایی همگرا و روایی واگرا استفاده شد. دربخش پایایی لازم است که پایایی در سطح معرف و متغیر پنهان بررسی شود. پایایی معرف از طریق سنجش بارهای عاملی و پایایی متغیرهای پنهان از طریق پایایی ترکیبی بررسی شد. با توجه به جدول (۵) مقدار آلفای کرونباخ برای همه متغیرها بزرگتر از حد مناسب ۰/۶ می‌باشد و از پایایی مطلوبی برخوردار می‌باشند. همچنین مقدار ضریب پایایی ترکیبی (ضریب دیلون-گلداشتاین) برای هر متغیر بیشتر از حد مطلوب ۰/۷ بوده و در نتیجه دلالت بر مناسب بودن پایایی ترکیبی هر متغیر دارد. معیار ارزیابی روایی همگرا به معنی میانگین واریانس مشترک بین متغیر پنهان و معرف‌هایش می‌باشد و حداقل مقدار قابل قبول برای آن ۰/۵۰ است. در این مدل روایی همگرای متغیرهای مدل همگی بالاتر از ۰/۵ بوده که همگی در سطح مناسب و قابل قبولی می‌باشند. از دیگر شاخص‌های روایی همگرا تحت عنوان قابلیت اطمینان، شاخص رائو از نظر هنسلر و همکاران می‌باشد که لازم است مقداری بالای ۰/۶ اختیار کند (نوروزی ۱۳۹۹). این شاخص نیز برای تمامی متغیرهای تحقیق بالاتر از حد مجاز بوده است.

جدول (۵) محاسبه آلفا کرونباخ، قابلیت اطمینان، پایایی ترکیبی و واریانس ابعاد و مولفه‌های پژوهش

	متغیرهای پنهان	آلفا کرونباخ CA>0/6	قابلییت اطمینان rho_A>0/7	پایایی ترکیبی CR>0/7	میانگین واریانس تبیین شده AVE>0/5
	تهدیدات سایبری	0/994	0/997	0/995	0/763
۱	آسیب‌پذیری‌های امنیتی	0/991	0/991	0/991	0/817
۱-۱	حفاظت ناکافی در مقابل شنود/ره‌گیری و بروز فعالیت مجرمانه	0/977	0/978	0/981	0/864
۱-۲	دسترسی فیزیکی غیرمجاز	0/937	0/944	0/96	0/888
۱-۳	ضعف در نگهداری منابع اطلاعاتی	0/974	0/974	0/978	0/866
۱-۴	نقص در زیرساخت‌های اطلاعاتی	0/964	0/964	0/97	0/821
۲	تهدیدات امنیتی	0/991	0/991	0/991	0/803
۲-۱	انسداد خدمت فعالیت مجرمانه	0/981	0/981	0/983	0/88
۲-۲	تهدیدات فیزیکی	0/955	0/956	0/971	0/918
۲-۳	خسارت‌های غیرعمدی	0/979	0/979	0/981	0/854
۲-۴	سوء استفاده	0/974	0/974	0/978	0/847
۳	عوامل انسانی	0/982	0/982	0/983	0/797
۳-۱	مدیریتی	0/967	0/967	0/973	0/836
۳-۲	کاربردی	0/971	0/972	0/976	0/834
۴	عوامل فرآیندی	0/981	0/981	0/982	0/775
۴-۱	قوانین	0/971	0/972	0/976	0/834

	متغیرهای پنهان	آلفا کرونباخ CA>0/6	قابلییت اطمینان rho_A>0/7	پایایی ترکیبی CR>0/7	میانگین واریانس تبیین شده AVE>0/5
۴-۲	نظارت	0/969	0/97	0/974	0/821
۵	عوامل فنی	0/965	0/991	0/969	0/719
۵-۱	برنامه‌ریزی	0/889	0/762	0/882	0/591
۵-۲	تجهیزات	0/98	0/981	0/983	0/865
۵-۳	رمز نگاری	0/982	0/982	0/985	0/89
۵-۴	پایش	0/887	0/905	0/902	0/535
۵-۵	کنترل دسترسی	0/981	0/982	0/984	0/883

محاسبه اعتبار واگرا (شاخص فورنل و لارکر- نسبت یکنواختی)

جدول‌های (۶) و (۷) روایی واگرای مدل پژوهش را نشان می‌دهد. روایی واگـرا، انـدازه‌ای اسـت که یک سازه به درستی از سایر سازه‌ها با معیار تجربی متمایز می‌شود. این روایـی در دو سـطح معرف و متغیر پنهان محاسبه می‌شود. در سطح معرف بـرای محاسـبه روایـی واگـرا، از بارهـای متقاطع استفاده می‌شود. برای بررسی روایی واگرا در سطح متغیر پنهان از نسبت یکنـواختی[1] و معیار فورنل-لارکر استفاده شد. هنسلر و همکاران بیان می‌کنند که ۰/۹۰ آستانه مطلـوب بـرای تایید روایی واگرا در نسبت یکنواختی می‌باشد. مقـادیر نسـبت یکنـواختی سـازه‌هـای مـدل در جدول (۷) نشان می‌دهند تمامی مقادیر از ۰/۹۰ پایین‌تر می‌باشند و روایـی واگـرا مـورد تاییـد می‌باشد. همچنین طبق شاخص فورنـل و لارکـر لازم اسـت کـه ریشـه دوم میـانگین واریـانس استخراج شده (AVE)، هر متغیر پنهان باید بیشـتر از بـالاترین همبسـتگی آن سـازه بـا سـایر سازه‌های مدل باشد، یعنی مقدار جذر میانگین واریانس استخراجی (AVE) متغیرهای پنهان در پژوهش حاضر که در خانه‌های موجود در قطر اصلی ماتریس قرار گرفته‌اند، از مقدار همبسـتگی میان آنها که در خانه‌های زیرین و چپ قطر اصلی ترتیب داده شده‌اند بیشتر باشد. منطـق ایـن سازه این است که یک سازه باید واریانس بیشتری با معرف‌های خود تا سایر سازه‌ها داشته باشد (Fornell & Larcker, 1981). نتایج جدول (۶) نشان می‌دهد که همه متغیرهـا روایـی واگـرای قابل قبولی دارند. به عنوان مثال ریشه دوم میانگین واریانس تبیین شـده بـرای متغیـر انسـداد

[1] Heterotrait-Monotrait Ratioo (HTMT)

خدمت فعالیت مجرمانه (۹۳/۸ درصد) شده است که از مقدار همبستگی این متغیر با سایر متغیرها بیشتر است.

جدول (۶) ضرایب همبستگی و شاخص اعتبار واگرا

	مولفه‌ها	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷
۱	انسداد خدمت فعالیت مجرمانه	۰.۹۳۸																
۲	برنامه‌ریزی	۰.۰۱۳	۰.۷۰۱															
۳	تجهیزات	۰.۶۸۳	۰.۲۱۱	۰.۹۳۰														
۴	تهدیدات فیزیکی	۰.۵۸۸	۰.۰۰۳	۰.۵۸۰	۰.۹۵۸													
۵	حفاظت ناکافی در مقابل شنود	۰.۵۹۵	۰.۰۰۴	۰.۴۸۱	۰.۶۹۰	۰.۹۲۹												
۶	خسارت‌های غیرعمدی	۰.۵۹۲	۰.۰۱۳	۰.۴۴۶	۰.۶۹۲	۰.۶۹۴	۰.۹۲۴											
۷	دسترسی فیزیکی غیرمجاز	۰.۵۹۰	۰.۰۰۲	۰.۴۸۱	۰.۵۸۵	۰.۶۹۱	۰.۴۹۱	۰.۹۴۲										
۸	رمز نگاری	۰.۵۸۲	۰.۱۵۹	۰.۵۹۵	۰.۴۷۹	۰.۶۸۱	۰.۴۸۴	۰.۵۷۸	۰.۹۴۳									
۹	سوء استفاده	۰.۵۸۹	۰.۰۰۸	۰.۴۷۸	۰.۴۸۵	۰.۶۹۲	۰.۴۹۰	۰.۵۸۸	۰.۵۷۸	۰.۹۲۰								
۱۰	ضعف در نگهداری منابع اطلاعاتی	۰.۵۹۴	۰.۰۱۵	۰.۴۸۴	۰.۴۸۹	۰.۶۹۵	۰.۴۹۳	۰.۵۹۳	۰.۵۸۳	۰.۳۹۱	۰.۹۳۰							
۱۱	قوانین	۰.۵۴۱	۰.۱۴۳	۰.۴۹۳	۰.۴۸۲	۰.۶۸۴	۰.۴۸۷	۰.۵۸۱	۰.۵۹۲	۰.۴۸۰	۰.۳۸۵	۰.۹۱۳						
۱۲	مدیریتی	۰.۵۹۱	۰.۰۲۴	۰.۴۸۱	۰.۴۸۵	۰.۶۹۲	۰.۴۹۱	۰.۴۸۷	۰.۵۵۸	۰.۴۹۱	۰.۳۹۱	۰.۳۸۲	۰.۹۱۴					
۱۳	نظارت	۰.۵۰۷	۰.۰۳۲	۰.۴۸۷	۰.۴۸۹	۰.۶۹۰	۰.۴۹۴	۰.۴۹۰	۰.۵۸۶	۰.۴۸۸	۰.۳۹۲	۰.۳۸۷	۰.۳۸۷	۰.۹۰۶				
۱۴	نقص در زیرساخت‌های اطلاعاتی	۰.۵۲۷	۰.۰۴۰	۰.۴۸۳	۰.۴۹۴	۰.۶۹۵	۰.۴۹۵	۰.۴۹۱	۰.۴۸۲	۰.۴۴۹	۰.۳۹۵	۰.۳۸۵	۰.۳۹۰	۰.۳۹۳	۰.۹۰۶			
۱۵	پایش	۰.۰۱۸	۰.۴۲۲	۰.۲۱۲	۰.۰۳۱-	۰.۰۰۳-	۰.۰۱۱-	۰.۰۱۹	۰.۲۱۱	۰.۰۰۷-	۰.۰۳۰-	۰.۲۱۳	۰.۰۲۵-	۰.۰۱۰-	۰.۰۲۶-	۰.۷۳۳		
۱۶	کاربردی	۰.۶۳۱	۰.۰۰۱-	۰.۴۸۲	۰.۴۸۹	۰.۶۹۵	۰.۴۹۳	۰.۴۹۱	۰.۴۸۳	۰.۴۹۲	۰.۳۹۵	۰.۳۸۴	۰.۳۹۱	۰.۳۹۲	۰.۴۹۵	۰.۰۲۷-	۰.۹۱۳	
۱۷	کنترل دسترسی	۰.۵۹۷	۰.۱۹۸	۰.۴۹۲	۰.۴۸۰	۰.۶۸۰	۰.۴۸۴	۰.۴۷۸	۰.۴۹۳	۰.۴۷۷	۰.۳۸۲	۰.۳۹۵	۰.۳۸۰	۰.۳۸۶	۰.۴۸۲	۰.۲۴۷	۰.۴۸۱	۰.۹۴۰

جدول (۷) مقادیر نسبت یکنواختی سازه‌های مدل

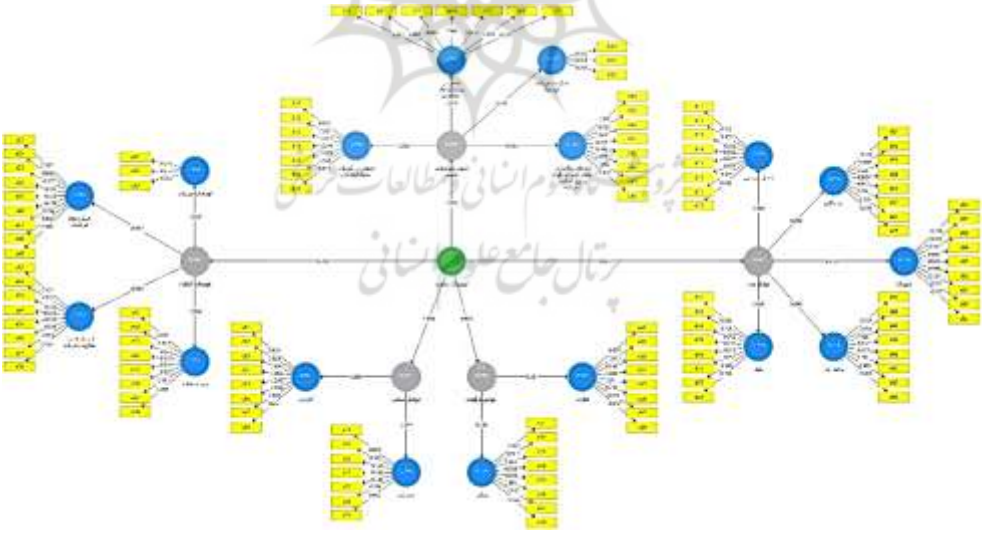
	مولفه‌ها	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷
۱	انسداد خدمت فعالیت مجرمانه																	
۲	برنامه‌ریزی	۰.۰۷۵																
۳	تجهیزات	۰.۴۲۳	۰.۰۸۲															
۴	تهدیدات فیزیکی	۰.۴۵۳	۰.۳۹۲	۰.۴۱۳														
۵	حفاظت ناکافی در مقابل شنود	۰.۴۸۶	۰.۴۱۵	۰.۴۱۵	۰.۴۶۴													
۶	خسارت‌های غیرعمدی	۰.۴۷۱	۰.۴۰۰	۰.۴۳۳	۰.۴۷۵	۰.۴۷۹												
۷	دسترسی فیزیکی غیرمجاز	۰.۴۶۸	۰.۳۸۷	۰.۴۱۹	۰.۴۶۷	۰.۴۷۶	۰.۴۷۳											
۸	رمز نگاری	۰.۴۱۹	۰.۳۶۵	۰.۴۸۴	۰.۴۰۸	۰.۴۱۲	۰.۴۳۰	۰.۴۰۳										
۹	سوء استفاده	۰.۴۵۳	۰.۴۱۲	۰.۴۰۰	۰.۴۴۳	۰.۴۷۲	۰.۴۶۱	۰.۴۶۰	۰.۴۰۰									
۱۰	ضعف در نگهداری منابع اطلاعاتی	۰.۴۸۰	۰.۳۹۱	۰.۴۲۹	۰.۴۶۲	۰.۴۸۶	۰.۴۷۴	۰.۴۸۵	۰.۴۲۴	۰.۴۶۷								
۱۱	قوانین	۰.۴۳۱	۰.۳۵۶	۰.۴۷۶	۰.۴۲۶	۰.۴۳۰	۰.۴۴۷	۰.۴۲۳	۰.۴۷۰	۰.۴۱۳	۰.۴۳۶							
۱۲	مدیریتی	۰.۴۵۸	۰.۴۰۹	۰.۴۱۵	۰.۴۴۱	۰.۴۷۲	۰.۴۶۸	۰.۴۵۶	۰.۴۱۱	۰.۴۶۷	۰.۴۷۱	۰.۴۲۳						
۱۳	نظارت	۰.۴۶۶	۰.۳۹۵	۰.۴۴۴	۰.۴۶۵	۰.۴۶۲	۰.۴۸۴	۰.۴۷۰	۰.۴۴۱	۰.۴۵۲	۰.۴۷۳	۰.۴۴۹	۰.۴۵۱					
۱۴	نقص در زیرساخت‌های	۰.۴۷۷	۰.۴۴۲	۰.۴۲۸	۰.۴۸۸	۰.۴۸۷	۰.۴۹۱	۰.۴۷۸	۰.۴۲۳	۰.۴۶۴	۰.۴۹۰	۰.۴۳۸	۰.۴۶۸	۰.۴۸۰				

	اطلاعاتی																	
۱۵	پایش	۰.۰۵۷	۰.۷۷۱	۰.۰۸۵	۰.۰۷۲	۰.۰۶۳	۰.۰۶۱	۰.۰۶۰	۰.۰۸۶	۰.۰۶۲	۰.۰۵۹	۰.۰۹۳	۰.۰۶۴	۰.۰۶۳	۰.۰۷۷			
۱۶	کاربردی	۰.۴۷۷	۰.۴۱۱	۰.۴۲۲	۰.۴۶۳	۰.۴۸۸	۰.۴۷۹	۰.۴۷۴	۰.۴۲۳	۰.۴۷۲	۰.۴۸۷	۰.۴۳۳	۰.۴۶۹	۰.۴۷۲	۰.۴۹۱	۰.۰۷۲		
۱۷	کنترل دسترسی	۰.۴۰۶	۰.۳۹۲	۰.۴۶۸	۰.۴۱۴	۰.۴۰۶	۰.۴۲۸	۰.۴۰۴	۰.۴۷۲	۰.۳۹۶	۰.۴۲۱	۰.۴۸۴	۰.۴۱۰	۰.۴۴۰	۰.۴۲۴	۰.۱۰۲	۰.۴۱۷	

در این پژوهش به دنبال طراحی ابزاری هستیم که با استفاده از آن ابعاد مختلف عوامل مورد بررسی را شناسایی کنیم. این ابزار مستخرج از پرسشنامه‌ای است که با استفاده از آن در جامعه مورد بررسی، میزان اثرگذاری آن ابعاد و مولفه‌ها را تعیین می‌کنیم. با توجه به اینکه در مرحله‌ی کیفی به کمک روش دلفی ابعاد و مولفه‌ها استخراج شده‌اند برای بررسی و تأیید ایده‌ها از تحلیل عاملی تاییدی برای وزن دهی به شاخص‌ها، مولفه‌ها و ابعاد پژوهش استفاده شده است.

تحلیل عاملی تاییدی، توانایی یک مدل از پیش تعیین‌شده در برازش به داده‌ها را سنجش می‌کند. به عبارت دیگر، تحلیل عاملی بررسی می‌کند آیا عامل‌هایی که در این پژوهش در نظر گرفته شده است، واقعاً واریانس‌های متغیرهای مشاهده‌شده را مطابق با الگوی تعیین‌شده تبیین می‌کنند یا خیر.

در این پژوهش از تحلیل عاملی تاییدی مرتبه دوم استفاده شده است و نتایج مطابق نمودار شکل (۱) بدست آمده است.



شکل (۱) تحلیل عاملی تاییدی مرتبه دوم ابعاد، مولفه‌ها و شاخص‌های پژوهش

نتیجه‌گیری و پیشنهاد

همان‌گونه که در مولفه "عوامل فرآینـدی" مشـهود اسـت، وزن مولفـه "قـوانین" از "نظـارت" بیشتر است به این معنی که نظارت هرچه دقیق بر اجـرای قـوانین نادرسـت کمکـی بـه بهبـود شرایط نمی‌کند، و با توجه اینکه مطابق جدول (۸)، مولفه قوانین با تمام مولفه‌های این پژوهش رابطه معنی‌دار و قوی دارد، بنابراین نه تنها خود قوانین از اهمیت ویژه‌ای برخوردار اسـت بلکـه " ارزیابی و به روزرسانی منظم قوانین، خط‌مشی و الزام" از اهمیت بالاتری برخوردار اسـت کـه در ادامه به بررسی رابطهٔ بین خط‌مشی، فرهنـگ سـازمانی و الگـوی صـحیح رفتـاری خـواهیم پرداخت. از این رو، تبیین قوانین برای اصلاح الگوی رفتاری کارشناسان امنیت اطلاعـات بسـیار حائز اهمیت است.

جدول (۸) شاخص‌ها و مولفه‌های بعد "عوامل فرآیندی"

عوامل فرآیندی	قوانین ۰/۹۶۸	E11	۰/۹۴۳	تدوین قوانین، خط‌مشی‌ها، دستورالعمل‌ها و الزامات
		E12	۰/۹۳۱	تدوین استانداردهای امنیتی
		E13	۰/۹۲۲	ارزیابی وبه روزرسانی منظم قوانین، خط‌مشی و الزام
		E14	۰/۹۱۳	طراحی معماری امن
		E15	۰/۹۱۳	تعیین راهبردهاواهداف مدیریتی براساس شرایط حاکم
		E16	۰/۹۱۰	روش شناسایی و طبقه‌بندی دارایی‌ها
		E17	۰/۸۹۲	برنامه‌ریزی تحلیل پیامد و بودجه‌بندی امنیتی
		E18	۰/۸۸۱	برنامه‌ریزی آموزشی و آگاهی رسانی امنیتی
	نظارت ۰/۹۶۷	E21	۰/۹۳۹	تدوین اصول و روال‌های پایش و کنترل کارمند
		E22	۰/۹۳۶	استفاده از چک لیست‌های امنیتی
		E23	۰/۹۱۸	تعیین جریمه برای عدم پیروی ازخط‌مشی‌های امنیت
		E24	۰/۹۱۵	اصول جمع‌آوری نظارت و تحلیل اطلاعات
		E25	۰/۹۱۵	روش‌های بررسی صحت، محرمانگی ودسترس پذیری
		E26	۰/۹۱۱	اصول طبقه‌بندی داده‌ها و منابع اطلاعاتی
		E27	۰/۸۳۶	رویه‌های تشخیص، گزارش دهی و پاسخ رخداد
		E28	۰/۸۴۹	عضویت وتعامل با انجمن‌های حرفه‌ای امنیت

همان‌طور که در مولفه "عوامل فنی" مشهود است، "تجهیزات" و "رمزنگـاری" وزن بـالاتری از "پایش" دارد و همچنین مطابق جدول (۶) "قوانین" همبستگی قـوی تـری بـا "تجهیـزات" و "رمزنگاری" دارد تا شاخص "پایش"، بنابراین این موضوع اثبات کننده آن است که با "پـایش" و "نظارت" نمی‌توان به یک سازمان امن رسید و یک بستر امن است کـه سـازمانی امـن ایجـاد می‌کند و در بستری ناامن انتظار سازمانی امن نمی‌توان داشت، بنابراین با فرهنگ‌سازی و ایجـاد الگوی رفتاری صحیح می‌توان به بستری امن رسید تا سازمانی امن شکل گیرد.

در مولفه "عوامل انسانی" مشخص گردید که شاخص‌های کاربردی وزن بالاتری از شاخص‌های مدیریتی دارد، بنابراین مطابق جدول (۹)، با بررسی مجدد مولفه عوامل انسانی دلیل این امر به این صورت برآورد گردید که مشخصه‌های کاربردی مستقیما با فرهنگ سازمانی رابطه مستقیم دارد و فرهنگ سازمانی با ایجاد الگوی رفتاری صحیح شکل می‌گیرد. و همچنین در مولفه مدیریتی نیز شاخص‌هایی که مستقیما با فرهنگ سازمانی و خط‌مشی مرتبط بوده‌اند نیز بالاترین وزن را داشته‌اند.

جدول (۹) شاخص‌های مولفه عوامل انسانی

عوامل انسانی	کاربردی ۰.۹۸۰	C11	۰/۹۳۲	همراهی کارکنان با خط‌مشی‌های امنیت اطلاعات سازمان	فرهنگ سازمانی
		C12	۰/۹۲۸	درک نیازهای امنیتی در سطوح مختلف سازمان	فرهنگ سازمانی
		C13	۰/۹۲۸	تعهد و وفاداری کارمندان به سازمان و ملاحظات امنیتی رایج	فرهنگ سازمانی
		C14	۰/۹۲۴	پیروی از استانداردها و دستورالعمل‌های امنیتی	فرهنگ سازمانی
		C15	۰/۹۲۲	رفتار محافظه کارانه کاربران در زمینه امنیت سیستم‌های اطلاعاتی	فرهنگ سازمانی
		C16	۰/۹۰۳	مهارت، تجربه، آگاهی و آموزش کاربران در زمینه امنیت اطلاعات	
		C17	۰/۸۹۱	حس پاسخگویی، خود ارزیابی و خود گزرش دهی	فرهنگ سازمانی
		C18	۰/۸۷۷	تعریف کاربری‌های مجاز سیستم و حقوق دسترسی	
	مدیریتی ۰.۹۷۴	C21	۰/۹۴۰	حاکمیت فرهنگ‌سازی همکاری در فعالیت و برنامه‌های امنیتی سازمان	
		C22	۰/۹۳۳	حمایت مدیریت عالی از برنامه‌ها، پروژه‌ها و خط‌مشی‌های امنیتی سازمان	
		C23	۰/۹۲۴	تدوین و اجرای برنامه‌های آموزشی و حوزه امنیت اطلاعات	
		C24	۰/۹۱۱	تشویق کارمندان به گزارش مخاطرات و مشکلات امنیتی	
		C25	۰/۹۰۶	تعیین مسولیت‌های امنیتی در سطح سازمان و استقرار سازمان امنیتی	
		C26	۰/۸۹۶	غربالگری و ارزیابی دوره‌ای کارمندان از منظر ملاحظات امنیت اطلاعات	
		C27	۰/۸۸۹	نظارت و پایش مستمر فعالیت‌هاب طرف ثالث در حوزه امنیت اطلاعات	

اولویت فرهنگ سازمانی به "مدیریت"، "پایش"، "نظارت" و "ارزیابی" به این دلیل است که عملا در یک شرکت داده محور بزرگ، نمی‌توان تمامی رفتارهای ریز و درشت کارشناسان امنیت اطلاعات را پایش کرد و کشف خطا، زمانی انجام می‌شود که خطا ایجاد شده باشد بنابراین ایجاد سازوکار جامع برای جلوگیری از خطاهای ناخواسته بسیار لازم و ضروری می‌باشد که برای این منظور، ایجاد یک فرهنگ سازمانی قوی، پاسخگو خواهد بود و این امر میسر نمی‌شود مگر با آموزش و بازآموزی الگوی صحیح رفتاری.

در مولفه "آسیب‌پذیری های امنیتی"، مشخصه "ضعف در نگهداری منابع اطلاعاتی" قویترین وزن را داشته است و مطابق جدول (۱۰)، با بررسی مجدد زیرشاخه‌های آن مشخص گردید "خط‌مشی و دستور العمل‌های ناکارآمد" در بین سایر گویه‌ها بالاترین وزن را داشته است.

جدول (۱۰) شاخص‌های مولفه "آسیب‌پذیری های امنیتی" مشخصه ضعف در نگهداری منابع اطلاعاتی

ضعف در نگهداری منابع اطلاعاتی	B11	۰/۹۴۶	خط‌مشی و دستور العمل‌های ناکارآمد
	B12	۰/۹۳۶	تفویض اختیار ناکارآمد
	B13	۰/۹۳۶	پیکربندی ضعیف سامانه
	B14	۰/۹۳۳	امکان تغییر در اطلاعات سامانه
	B15	۰/۹۳۱	ارزیابی امنیتی ناکارآمد فناوری‌ها
	B16	۰/۹۲۶	امکان دسترسی غیر مجاز
	B17	۰/۹۰۴	مدیریت خطا به شیوه نادرست

بدیهی است که خط‌مشی امنیت اطلاعات یک شرکت داده محور باعث ایجاد فرهنگ سازمانی آن شرکت شده و ایجاد الگوی صحیح رفتاری برگرفته از تصحیح خط‌مشی امنیت اطلاعاتی خواهد بود(رجبی و علیپور، ۱۴۰۱).

برای بسیاری از سازمان‌ها و مؤسسات اهمیت و ضرورت خط‌مشی‌های امنیت اطلاعات هنوز در هاله‌ای از ابهام قرار دارد و برخی دیگر امنیت را تا سطح یک محصول تنزل داده و فکر می‌کنند که با تهیه یک محصول نرم افزاری خاص و نصب آن در سازمان خود، امنیت را برای سازمان خود به ارمغان می‌آورند. وجود یک شکاف و یا مشکل امنیتی، می‌تواند یک سازمان را به روش‌های متفاوتی تحت تأثیر قرار دهد. آشنایی با عواقب خطرناک یک حفره امنیتی در سازمان و شناسایی مهمترین تهدیدات امنیتی که می‌تواند حیات یک سازمان را با مشکل مواجه نماید، ازجمله موارد ضروری به منظور طراحی و پیاده‌سازی یک مدل امنیتی در یک سازمان است. برای تبیین مبانی نظری و اثبات نتایج، مطابق جدول ۱۰ نتایج حاصله از این پژوهش با نتایج حاصله از پژوهش شعبانی ۱۴۰۰ نیز مورد مقایسه قرار گرفت و نتیجه حاصل از این مقایسه تایید کننده استدلال‌ها و مبانی نظری این پژوهش می‌باشد.

جدول (۱۱) مقایسه نتایج این پژوهش با پژوهش شعبانی ۱۴۰۰ و حسینی ۱۳۹۳

محمدمهدی شعبانی (۱۴۰۰)		این پژوهش			حسینی (۱۳۹۳)	
رتبه میانگین	مولفه	مولفه		وزن مولفه عاملی دو مرحله ای	رتبه	مولفه
16. 26	فرهنگ‌سازمانی	فرهنگ سازمانی	خط‌مشی و دستور العمل ها	0. 946	۲	فرهنگ و بافت سازمانی
13	ساختارسازمانی	ساختار سازمانی	تدوین قوانین، خط‌مشی‌ها، دستورالعمل‌ها و الزامات	0. 943	۴	عوامل ساختاری

محمدمهدی شعبانی (۱۴۰۰)		این پژوهش			حسینی (۱۳۹۳)	
رتبه میانگین	مولفه		مولفه	وزن مولفه عاملی دو مرحله ای	رتبه	مولفه
			حاکمیت فرهنگ‌سازی همکاری در فعالیت و برنامه‌های امنیتی سازمان	0. 94		
			حمایت مدیریت عالی از برنامه‌ها، پروژه‌ها و خط‌مشی‌های امنیتی سازمان	0. 933		
12. 11	منابع انسانی	منابع انسانی	همراهی کارکنان با خط مشی‌های امنیت اطلاعات سازمان	0. 932	۱	عوامل سازمانی
			درک نیازهای امنیتی در سطوح مختلف سازمان	0. 928		
			تعهد و وفاداری کارمندان به سازمان و ملاحظات امنیتی رایج	0. 928		
			پیروی از استانداردها و دستورالعمل‌های امنیتی	0. 924		
			رفتار محافظه کارانه کاربران در زمینه امنیت سیستم‌های اطلاعاتی	0. 922		
			حس پاسخگویی، خود ارزیابی و خود گزرش دهی	0. 891		
10. 98	آموزش و بازآموزی	آموزش	مهارت، تجربه، آگاهی و آموزش کاربران در زمینه امنیت اطلاعات	0. 903	۳	خط‌مشی سازمانی

از این رو مدیران و کارشناسان امنیت سازمان وظیفه دارند تا با تدوین استانداردها و خط مشی‌های امنیت، از اطلاعات در برابر تهدیدات پاسداری و حفاظت نموده و همچنین با تدوین خط‌مشی‌های امنیت اطلاعات دسترس پذیری، جامعیت، محرمانگی منابع اطلاعاتی سازمان را تضمین نمایند.

پاسخ به سؤال محوری این پژوهش

- تا چه حد، رابطه‌ای بین خط‌مشی و فرهنگ سازمانی و الگوی صحیح رفتاری کارشناسان امنیت اطلاعات نسبت به امنیت اطلاعات وجود دارد؟

منشاء خط‌مشی یک سازمان قوانین آن سازمان است و نتیجه خط‌مشی، رسیدن به اهداف سازمان می‌باشد و وزن بالای شاخص "قوانین" در مولفه "عوامل فرایندی" و لزوم بروز رسانی خط‌مشی که جزو مشخصه‌های شاخص "قوانین"

می‌باشد نشان دهنده اهمیت خط‌مشی و فرهنگ سازمانی است و وزن بالای شاخص‌های مربتط با فرهنگ سازمانی در بعد " عوامل انسانی" نشانگر رابطه مستقیم و تاثیر گذار فرهنگ سازمانی بر الگوی رفتاری کارشناسان امنیت اطلاعات می‌باشد، بنابراین خط‌مشی و فرهنگ سازمانی نقش بسزایی در تصحیح یا تخریب الگوی رفتاری کارشناسان امنیت اطلاعات و در نتیجه در عملکرد سازمان دارد و خطاهای خط‌مشی امنیت اطلاعات می‌تواند مستقیما بر روی عملکرد و اهداف سازمان تاثر بگذارد.

قدردانی

از تمامی خبرگان و اساتیدی که دانش خویش را سخاوتمندانه در اختیار محققان این پژوهش قرار دادند، کمال تشکر را داریم.

منابع

- حسینی، سیدصمد، حبیبی، حمداله، و حسن‌پور، محمد. (۱۳۹۳). مدل استرس شغلی در محیط‌های آموزشی - دانشگاهی. *پژوهش‌های نوین روانشناختی (روانشناسی دانشگاه تبریز)*، *۹(۳۳)*، ۶۱-۸۹. *SID*
- خطایی, ناهید؛ هدایتی, علیرضا, و آغازاریان, واهه. (۱۴۰۱). بررسی روش‌های مقابله با حملات جعل در ارتباطات شبکه‌های خودرویی. *نشریه"فناوری اطلاعات و ارتباطات انتظامی*", doi: 10. 22034/pitc. 2022. 1269297. 1153
- دی پیر, محمود. (۱۴۰۱). ارائه معیاری برای محاسبه خطر امنیتی لینک‌ها برای جلوگیری از کلاهبرداری‌های اینترنتی. *نشریه فناوری اطلاعات و ارتباطات انتظامی*. doi: 10. 22034/pitc. 2022. 1270147. 1167
- رجبی فرجاد, حاجیه؛ علیپور, علی رضا. (۱۴۰۱). تاثیر اجرای خط‌مشی‌گذاری عمومی بر فرهنگ سازمانی. *خط‌مشی‌گذاری عمومی در مدیریت*. doi: 10. 30495/ijpa. 2022. 66807. 10867
- قربانی، ولی اله و ثقفی، کامیار، (۱۳۹۸)، ارائه مدل کلان امنیت اطلاعات فضای سایبر در جمهوری اسلامی ایران، *فصلنامه امنیت ملی*.

- کریمی, و پیکری. (۱۳۹۸). مدیریت امنیت اطلاعات: تاثیر تعهد سازمانی و عواقب ادراک‌شده افشای اطلاعات محرمانه بر قصد نقض امنیت اطلاعات بیماران. *اخلاق پزشکی*, ۴۴(۱۳), ۲۰-۲۹.
- منصوری علی و جعفری علی، (۱۳۹۴). *نقش آموزش‌های تخصصی IT در پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سازمان*. دومین همایش ملی علوم مدیریت و برنامه‌ریزی آموزش و استانداردسازی ایران.
- نوروزی, حسین؛ سمیعی, محمد و رشنوادی, یعقوب. (۱۳۹۹). *شناسایی و تبیین راهبردهای ترفیع در رسانه‌های اجتماعی (مورد مطالعه: اینستاگرام)*. تحقیقات بازاریابی نوین. doi: 10.22108/nmrj. 2020. 123203. 2133
- Ahmed, S. , & Hassan, M. (2003). Survey and case investigations on application of quality management tools and techniques in SMIs. *International Journal of Quality & Reliability Management*, *20*(7), 795-826.
- AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in human behavior*, 49, 567-575.
- Ali, R. F. , Dominic, P. D. D. , Ali, S. E. A. , Rehman, M. , & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, 11(8), 3383.
- Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, 102003.
- Ansari, M. F. , Sharma, P. K. , & Dash, B. (2022). Prevention of phishing attacks using AI-based Cybersecurity Awareness Training. *Prevention*.
- Chen, X. , & Tyran, C. K. (2023). A Framework for Analyzing and Improving ISP Compliance. *Journal of Computer Information Systems*, 1-16.
- Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days? *Information security technical report*, 14(4), 186-196.
- Deal, T. & Kennedy, A. (1999). The New Corporate Cultures: Revitalizing the workplace after Downsizing, Mergers, and Reengineering. *Cambridge: Basic Books*, a member of the Perseus Books Group
- Ernest Chang, S. and Lin, C. (2007), Exploring organizational culture for information security management, *Industrial Management & Data Systems*, Vol. 107 No. 3, pp. 438-458. https: //doi. org/10. 1108/02635570710734316
- Fornell, C. , & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, 18(1), 39-50.

- Karlsson, M. , Karlsson, F. , Åström, J. and Denk, T. (2022), The effect of perceived organizational culture on employees' information security compliance, *Information and Computer Security*, Vol. 30 No. 3, pp. 382-401. https: //doi. org/10. 1108/ICS-*06-2021-0073*
- Moti Zwilling et al. (2022). "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study", *Journal of Computer Information Systems* Volume 62, - Issue 1
- Niekerk, J. v. , & Solms, R. v. (2005). A holistic framework for the fostering of an information security sub-culture in organizations. *Nelson Mandela Metropolitan University*.
- Parsons, K. M. , Young, E. , Butavicius, M. A. , McCormac, A. , Pattinson, M. R. , & Jerram, C. (2015). The Influence of Organizational Information Security Culture on Information Security Decision Making. *Journal of Cognitive Engineering and Decision Making*, 9(2), 117–129. https: //doi. org/10. 1177/1555343415575152
- Rahimli, Ailar. (2012). Knowledge Management and Competitive Advantage. *Information and Knowledge Management*. 37-43.
- Solomon, G. and Brown, I. (2021), The influence of organisational culture and information security culture on employee compliance behaviour, *Journal of Enterprise Information Management*, Vol. 34 No. 4, pp. 1203-1228. https: //doi. org/10. 1108/JEIM-08-2019-0217
- Stanton, J. , Mastrangelo, P. , Stam, K. , & Jolton, J. (2004). *Behavioral information security: Two end user survey studies of motivation and security practices.*
- Tejay, G. P. , & Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management*, 60(3), 103751.
- Xiaofen Ma, (2022) "IS professionals' information security behaviors in Chinese IT organizations for information security protection", *Information Processing & Management*.

پیوست ۱ کدگذاری منابع فارسی و خارجی پژوهش استفاده شده در روش فراترکیب

پژوهشگر	متون انتخابی	کد منبع
زینب محمدصادقی	جاسوسی سایبری و ضرورت مقابله با آن	S1
نوروز پورقهرمانی	چگونگی سلطه‌گری دشمن بر شریانهای اطلاعاتی در فضای سایبری، تدابیر و راهکارهای مقابله با آن	S2
وحید عابدینی یزدی	پدافند غیرعامل، بررسی تهدیدات سایبری و راهکارهای مقابله با آن	S3
نادر ایرانپور	مدل مفهومی پیادهسازی موفق سیستم مدیریت امنیت اطلاعات	S4
علی اکبر عیسی زاده	شناسایی و رتبه بندی عوامل برون سازمانی موثر در پیاده سازی سیستم مدیریت امنیت اطلاعات	S5
فاطمه آناهید	ابعاد حقوقی جرم‌های سایبری و راهکارهای هقابله با آن	S6
علی اکبر عیسی زاده	شناسایی و رتبه بندی عوامل فناوری و تکنولوژی موثر درپیاده سازی سیستم مدیریت امنیت اطلاعات	S7
رویا محمودآباد	ضرورت پیاده‌سازی سیستم مدیریت امنیت اطلاعات در دولت الکترونیک	S8
امیرهوشنگ تاج فر	رتبه بندی موانع پیاده سازی سیستم مدیریت امنیت اطلاعات و بررسی میزان آمادگی مدیریت اکتشاف	S9
علی عبداله خانی	سنجش تهدیدات سایبری	S10
علی پور رکن آبادی	تهدیدات سایبری و تأثیر آن بر امنیت ملی	S11
فاطمه مینوئی مقدم	بهبود رو شهای کشف تهدیدات سایبری د ر شبکه‌های اجتماعی با استفاده از الگوریت مهای داده کاو ی	S12
زهرا غلامی	اهمیت وچالش‌های امنیت اطلاعات وسیستم مدیریت امنیت اطلاعات (ISMS)برای سازمان‌ها	S13
علیرضا علیزاده	فرماندهی و کنتر ل انواع تهدیدات در دفاع سایبری با رویکردی درحوزه پدافند غیرعام ل در سازمان ها	S14
محمد رضا عیوضی	انواع تهدیدات در فضای سایبری و راهکارهای مقابله با آن	S15
مینا سهرابی	ارائه روشی نوین برای تشخیص نفوذ در سیستم های پایگاه داده ای به کمک مفاهیم داده کاوی	S16
محمدحسین قیامتیون	تشخیص نفوذ با استفاده از روشهای داده کاوی	S17
سمانه جدائی	تشخیص نفوذ در پایگاه داده و شبکه با استفاده از تکنیک‌های داده کاوی مبتنی بر الگوهای رفتاری کاربران	S18
ایوب صفائی شکرانلو	ارائه یک روش بهبود یافته جهت تشخیص نفوذ در شبکه با استفاده از الگوریتم‌های داده کاوی	S19
هاشم میربهاری	شناسائی و مقابله با حملات دورن سازمانی در پایگاه‌های داده‌ای رابطه‌ای	S20
مرجان رئیسی استبرق	تشخیص نفوذ با استفاده از راهکارهای مبتنی بر یادگیری ماشینی	S21
زهرا صالحی	شناسایی بدافزارها با استفاده از الگوهای رفتاری	S22
عادل قاسمی مرزبالی	بررسی مدیریت امنیت اطلاعات در ددانشگاه هرمزگان و ارائه راه کارهای ارتقای آن	S23
سیده صبا باقری	شناسایی موانع پیاده سازی سیستم مدیریت امنیت اطلاعات در شرکت‌های ایرانی	S24
سحر میرانوری	شناسایی و اولویت بندی عوامل کلیدی موفقیت در اجرای سیستم مدیریت امنیت اطلاعات در سازمان های ایرانی	S25
نوید آفتابی	یک مدل مدیریت امنیت اطلاعات برای کاهش ریسک‌های احتمالی در سازمان‌های مبتنی بر فناوری اطلاعات	S26

محبوبه باغبانزاده	شناسایی و اولویت بندی عوامل انسانی موثر بر امنیت اطلاعات با استفاده از رویکرد ترکیبی AHP	S27
همایون شیروانی	لزوم پیاده‌سازی سیستم امنیت اطلاعات در سازمان ها	S28
حمیدرضااسماعیل پور	شناسائی و رتبه‌بندی عوامل و شاخصهای کلیدی موثر بر بهبود سیستم مدیریت امنیت اطلاعات	S29
کیانا عباسی	عوامل تأثیرگذار بر تسهیم دانش امنیت اطلاعات در سازمان (مورد مطالعه: بانک توسعه صادرات ایران)	S30
فاطمه محبوبی راد	بهبود امنیت اطلاعات با استفاده از داده کاوی	S31
احمد رضا نوروزی	تحلیل و همبسته‌سازی هشدارها و گزارش‌های امنیتی با استفاده از داده کاوی	S32
فریده اسفندیاری	طراحی سامانه تشخیص نفوذ بر اساس ترکیب روشهای داده کاوی، شبکه عصبی و انتخاب ویژگی	S33
امیر مسعود بایبوردی	پیش‌بینی و بررسی الگوهای رفتاری مالکین شهر تبریز با استفاده از داده کاوی	S34
سهیلا عاشوری زاده	رابطه فرهنگ سازمانی با مدیریت امنیت اطلاعات در بانک ملی ایران	S35
صدیقه نوروزیان	رویکرد چندبعدی به ریسک مدیریت امنیت اطلاعات با استفاده از FMEA فازی	S36
محمد قمبرپورایور	شناسایی و بررسی عوامل موثر بر ارتقاء عملکرد مدیریت امنیت اطلاعات با رویکرد مدیریتی	S37
فرح نقی لو	بررسی عوأمل کلیدی موفقیت پیادسازی سیستم مدیریت امنیت اطلاعات در دانشگاههای دولتی ایران	S38
حمید خواجویی	مطالعه کنترل‌های امنیت اطلاعات بر اساس استانداردهای بین المللی	S39
محسن نیک پور	بررسی عوامل کلیدی موفقیت در ایجاد سیستم مدیریت امنیت اطلاعات در سازمان امور مالیاتی کشور	S40
مهدی احمدی جزنی	بررسی فرهنگ سازمانی و تاثیر آن بر مدیریت امنیت اطلاعات با توجه به سطح آمادگی کارکنان قوه قضاییه	S41
ملیکا ارمندئی	طراحی و پیاده‌سازی سیستم خبره ضریب دار سلسله مراتبی جهت ارزیابی امنیت اطلاعات سازمان مبتنی بر استاندارد بین المللی ایزو	S42
مسعود زندی فرد	ارائه مدل امن رایانش ابری با هدف کاهش چالش‌های مدیریتی و امنیتی	S43
سحر آریا خصال	ارزیابی آمادگی سازمانی برای استقرار سیستم مدیریت فرایند کسب و کار با مدل ترکیبی	S44
مهسا جعفری خوزانی	ارائه یک راهکار برای تشخیص رویداد در سامانه‌های اطلاعاتی با استفاده از الگوریتم‌های یادگیری ماشین	S45
کوروش نظری	شناسایی و تحلیل ریسک امنیت اطلاعات با رویکرد منطق فازی در شرکت آلومینای ایران	S46
حسین حسین زاده	الگویی جهت ارزیابی آمادگی سازمان برای پیاده سازی امنیت برنامه های کاربردی بر اساس استاندارد جهانی ایزو ۱-۲۷۰۳۴	S47
علی جعفری	بررسی و اولویت‌بندی نقش آموزش و عوامل مؤثر در مقابله با تهدیدات فضای تبادل الکترونیکی در سازمان با رویکردFAHP	S48
مسلم خاکبیز	شناسایی و اولویت‌بندی عوامل مؤثر بر امنیت سیستمهای اطلاعاتی سازمان با استفاده از مدلهای تصمیم گیری چند شاخصه	S49
ژاله داوری	ارزیابی مدلهای امن‌سازی ذخیره اطلاعات در پایگاه داده‌های بزرگ	S50
کیانا عباسی	عوامل تأثیرگذار بر تسهیم دانش امنیت اطلاعات در سازمان (مورد مطالعه: بانک توسعه صادرات ایران)	S51

S52	بررسی تاثیر پیاده سازی سیستم مدیریت امنیت اطلاعات بر ارتقا و تداوم سیستمهای اطلاعاتی و خدمات فناوری اطلاعات	احمد صالحی
S53	ارائه الگوی امنیت در فضای سایبر جمهوری اسلامی ایران با رویکرد آینده پژوهانه	امیرحسین مقدسی
S54	ارائه مدل مفهومی همکاری‌های بین المللی با رویکرد تقویت دفاع سایبری کشور(بر اساس نظریه پردازی داده بنیاد)	مهراب رامک
S55	احصاء، ارزیابی و تحلیل شکاف ابعاد نظام رصد، پایش و هشداردهی سایبری از منظر امنیت ملی	محمدرضا ولوی
S56	ارائه مدل فرایندی دفاع سایبری بومی	حسین امیرلی
S57	تبیین نقش شبکه ملی اطلاعات در مدیریت فرصتها و تهدیدهای فضای مجازی کشور	داود عبیری
S58	ارائه یک مدل برای بهبود مدیریت امنیت دارایی های اطلاعاتی سازمان در سیستم مدیریت امنیت اطلاعات ادارات	فاطمه خضری پور
S59	ارائه روشی مناسب برای بهبود و توسعه شاخصهای مدیریت امنیت اطلاعات جهت طراحی و پیادهسازی در سازمان‌ها	مجتبی بهرامی
S60	ارزیابی و رتبه‌بندی عوامل موثر در اشتراک گذاری دانش امنیت اطلاعات بر اساس مدل ترایاندیس	مهدی صائمیان
S61	آشکارسازی ناهنجاریهای سایبری براساس روشهای داده کاوی و یادگیری ماشین	مریم فروتنی
S62	تحلیل و رتبه‌بندی عوامل مؤثر بر مدیریت ریسک‌های سایبری در ایران	کیومرث قلاوند
S63	طراحی مدل مطلوب امنیت فناوری اطلاعات در پالایشگاه گاز ایلام: مدلی برآمده از نظریه داده بنیاد	فاطمه نرگسی
S64	بررسی تأثیر آموزش بر ارتقای امنیت اطلاعات در سازمان‌های دولتی	طاهره صیدی
S65	اولویت‌بندی عوامل مؤثر بر مدیریت امنیت فناوری اطلاعات(سازمان ثبت احوال شهرستان ایلام)	میترا تخمار
S66	ارائه راهکاری بومی و عملیاتی جهت رفع آسیب‌پذیری و تهدیدات امنیتی شبکه‌های کامپیوتری سازمانی	نورالله آزادبیگی
S67	تحلیل میزان وقوع جرایم رایانه‌ای و عوامل موثر بر آن با استفاده از تکنیک داده کاوی	امیددوستمحمدی
S68	شناسایی و رتبه‌بندی عوامل مؤثر بر رفتار امنیت اطلاعاتی کارکنان در شبکه‌های اجتماعی سازمان هواپیمایی کشوری	محمد محمدی
S69	عوامل موثر در پذیرش سیاست‌های امنیت اطلاعات توسط کارمندان در سازمان	اقدس اسفدیار
S70	شناسایی و الویت بندی شاخص های ارزیابی ریسک امنیت اطلاعات (اداره ثبت احوال استان تهران)	فرید حیدری
S71	واکاوی جایگاه بعد دانشی در الگوهای معماری سازمانی (مطالعه موردی: سازمان‌های امنیتی)	جعفر فینی زاده
S72	ارائه مدلی هوشمند برای سنجش امنیت اطلاعات درسازمان‌ها با استفاده ازمنطق فازی (مطالعه موردی شرکت پالایش گاز پارسیان)	مجید نادری بنی
S73	الگوی راهبردی حفاظت سایبری از زیرساخت‌های اطلاعاتی حیاتی جمهوری اسلامی ایران	رضا تقی پور
S74	ارائه مدل مفهومی ارزیابی تهدیدات تروریسم سایبری	حسین امیرلی
S75	ارائه مدل تحول در چرخه‌های ظهور بحران‌های سیاسی- امنیتی، متأثر از فضای سایبر	حمید رضا شجاع
S76	متولیان تأثیرگذار بر فرآیند ایجاد قدرت بازدارندگی و پیشگیری از تهدیدات و حملات سایبری در نظام دفاع سایبری	علی ملائی
S77	طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران	رضا تقی پور

S78	الگوی بازدارندگی در فضای سایبر بر اساس نظریه بازی‌ها در راستای تأمین امنیت دارایی‌های سایبری	علی ملائی
S79	الگوی راهبردی صیانت امنیتی فضای سایبر نیروهای مسلح به‌منظور خنثی‌سازی تهدیدات و صیانت از فضای سایبر نیروهای مسلح	ابراهیم محمودزاده
S80	همگرایی جنگ الکترونیک و جنگ سایبری و الزامات اجرای آن در سازمان‌های نظامی	احمدرضا فرحبخت
S81	جداسازی حملات در سامانه‌های تشخیص نفوذ با استفاده از فنون ماشین بردار پشتیبان شبکه‌های عصبی خودسازمان ده	محمد نظری فرخی
S82	بررسی عوامل رفتاری مؤثر بر حمایت کارکنان از خط‌مشی‌های حفظ اطلاعات	علی چیت ساز
S83	ارائه مدل فرایندی دفاع سایبری بومی	مهراب رامک
Source code	**Selected texts**	**Researcher**
S84	A Survey of Security in MultiAgent Systems. Sciencedirect, Expert Systems with Applications	Carneiro Cavalcante
S85	System Integration and Security of Information Systems. Sciencedirect, Procedia Computer Science	Boiko, Andrii
S86	Security in Information System: Advances and New Challenges. Journal of Computer Standards & Interfaces	Blanco, Carlos, Rosado
S87	Vulnerabilities in Network Infrastructures and Prevention/ Containment Measures. Proceedings of Information Science & IT Education Conference (InSITE)	Awodele, Oludele
S88	How to Model a Aeure Information System: A Case Study, Internationa Journal of Information and Education Technology	Alotaibi, Youseef
S89	Information Systems Threats and Vulnerabilities. International Journal of Computer Applications	Alghazzawi
S90	Accident Prevention and Management of Information Systems Security in Technology-Based Work Processes, Journal of Loss Preventation in The Process Industries	Albrechtsen
S91	An Information Security Risk-Driven Investment Model for Analysing Human Factors. Emeraldinsight, Information and Computer Security	Alavi, Reza
S92	Cyber Security and The Internet of Things (IoT): Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security	Abomhara, Mohamed
S93	An Overview of Social Egineering Malware: Trends, Tactics and Implications. Sciencedirect, Technology in Society	Abraham, Sherly
S94	The Quest for Complete Security: An Emprical Analysis of Users' Multi-Layered Protection From Security Threats. Springer, InfSyst Front	Crossler, Robert E
S95	Enterprise Information Systems Security: A Case Study in The Banking Sector. International Federation for Information Processing, LNBIP	Chaudhry, Peggy E
S96	Modeling and Assessing The Impact of Security Attacks on Enterprise Information Systems, Springer International Publishing Switzerland, LNBIP	Djemaiel
S97	Monitoring Physical Threats in The Data Center, Schneider Electric's Data Center Science Center. • Dang, Khanh & Dang, Tri	Cowan, Christian
S98	General Deterrence Theory: Assessing Information Systems Security Effectiveness in Large Versus Small Business University of North Texas, Theses	Chuessler, Josef H
S99	ecurity Threats on Cloud Computing Vulnerabilities.	Chou, Te-Shun

	International Journal of Computer Science & Information Technology (IJCSIT)	
S100	Understanding the Violation of IS Security Policy in Organizations: An Integrated Model Based on Social Control and Deterrence Theory. Sciencedirect, Computers & Security	Cheng, Lijiao
S101	Investigating Perceived Security Threats of Computerized Accounting Information Systems: An Emprical Research. Emeraldinsight, Journal of Economic and Administrative Sciences	Hayale, Talal H
S102	A Conceptual Framework for Information	Paul
S103	The Role of External and Internal Influences on Information Systems Security- A Neo-Institutional Perspective. Sciencedirect, Journal of Strategic Information Systems	Hu, Qing, Hart
S104	Inforrmation Systems Security Audit: An Ontological Framework, ISACA Journal	Gebremedhin Kassa
S105	Information System Security Threats Classifications. Journal of Information and Organizational Sciences	Geric, Sandro
S106	Security-Related Behavior in Using Information Systems in The Workplace: A Review and Synthesis, Sciencedirect, Computers & Security	Guo, Ken H
S107	Impacts of Organizational Capabilities in Information Security. Emeraldinsight, Information Management and Computer Security	Hall, Jacqueline H
S108	Security Awareness, Assessment and Training. Elsevier, Emerging Trends in ICT Security, Chapter	Brewster, Ben
S109	A Vulnerability-Centric Requirements Engineering Framework: Analyzing Security Attacks, Countermeasures and Requirements Based on Vulnerabilities. Springer, Requirements Eng	Elahi, Golnaz
S110	Security Issues in Cloud Environments: A Survey, International Journal Information Security	Fernandes, Diogo
S111	Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective. Sciencedirect, Computers in Human Behavior	Gamagedara Arachchilage
S112	Modeling and Assessing the Impact of Security Attacks on Enterprise Information Systems, Springer International Publishing Switzerland, LNBIP	Djemaiel, Yacine

پرتال جامع علوم انسانی